IMES DISCUSSION PAPER SERIES

最近の金融業務における情報セキュリティ評価・認定を巡る動向について

うね まさし　なかはら しんいち
宇根正志・中原慎一

Discussion Paper No. 99-J-44

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES
BANK OF JAPAN

日本銀行金融研究所

〒103-8660 日本橋郵便局私書箱 30 号

IMES Discussion Paper Series 99-J-44
1999 年 11 月

最近の金融業務における情報セキュリティ評価・認定を巡る動向について

うね まさし　　なかはら しんいち
宇根正志*1・中原慎一*2

要　旨

インターネットを利用したオンラインバンキングやオンライン証券取引等、オープンなネットワークを活用した新しい金融サービスを提供する金融機関が増えており、金融ネットワークのオープン化が進展している。このため、金融分野では、暗号技術等を利用した情報セキュリティ対策の実施が喫緊の課題として位置付けられている。

金融機関が情報セキュリティ対策を検討する場合、ISO や IEC 等の国際標準化団体によって策定された標準規格や技術文書が参考になる。例えば、欧米では、金融業務における情報セキュリティガイドライン ISO/TR 13569 は、金融機関による情報セキュリティ対策に関する有用な指針として利用されている。

最近では、第三者機関による情報セキュリティ製品・システムやその管理・運用体制に対する評価・認定の枠組みが整備されつつある。情報セキュリティ製品やシステムの評価基準 ISO/IEC 15408 が 1999 年 6 月に国際標準化されており、現在 ISO/IEC 15408 に基づく評価スキームとして CEM の検討が進められている。

また、情報セキュリティ管理に第三者機関による評価制度を導入した、英国の情報セキュリティガイドラインである BS 7799 は、従来から欧州の金融機関をはじめとして幅広く利用されていたが、1998 年には、BS 7799 に基づく評価・認定スキームとして c:cure が発足している。

このように、情報セキュリティに関するガイドラインに加えて、情報セキュリティ製品・システムやその管理・運用体制に対する評価・認定の枠組みが整備されつつある。情報セキュリティ評価・認定のスキームは、企業が情報システムのセキュリティ対策を検討する際の有効な手段であり、今後幅広い分野において利用されるようになると考えられる。金融分野においても、有効なセキュリティ対策の実現に向けて、情報セキュリティ評価・認定のスキームを活用していくことも考えられる。

キーワード：情報セキュリティ、国際標準、ISO/TR 13569、ISO/IEC 15408、BS 7799、コモンクライテリア、CEM、c:cure
JEL Classification：L86、L96、Z00

*1 日本銀行金融研究所研究第 2 課（E-mail: masashi.une@boj.or.jp）
*2 日本電信電話情報流通プラットフォーム研究所（E-mail: nakahara@dsa.isl.ntt.co.jp）

本論文は、1999 年 11 月 1 日に日本銀行で開催された「第 2 回情報セキュリティシンポジウム」への提出論文に加筆・修正を施したものである。

目　次

頁

Ⅰ. はじめに

近年のインターネットの急速な拡大に伴って、オープンなネットワークを利用した新しい金融サービスに対するニーズが高まっており、インターネットを利用したオンラインバンキングやオンライン証券取引等のサービスを開始する金融機関が増えている。また、最先端のインターネット技術によって金融機関内部のネットワークを再構築し、業務の一層の効率化を図る動きもみられている。この結果、従来、物理的にもプロトコルとしても外部から隔離されていた金融ネットワークが、外部のネットワークと接続する動き ― 金融ネットワークのオープン化 ― が拡大している。

こうした金融ネットワークのオープン化により、金融機関による暗号技術等を活用した情報セキュリティ対策が喫緊の課題となっている。従来は、クローズドな（閉じた）ネットワークを前提とした金融情報システムセンターの安全対策基準等が利用されてきたが、今後金融機関が情報セキュリティ対策を実施する際には、①暗号技術等に代表される情報セキュリティ技術の評価が必要であるほか、②国際的な情報セキュリティレベルの整合性も考慮することが必要となる。こうした課題をクリアするために、ISO や IEC 等の国際標準化団体が策定した標準規格や技術報告書の重要性が増している。

一般に、適切な情報セキュリティ対策を実行するためには、次の一連の手続きが必要といわれている。

(A)組織の情報技術戦略に基づき、何をどのように保護するかを定めた情報セキュリティポリシーを作成する。
(B)情報セキュリティポリシーに基づき、具体的な情報管理の方法を規定する情報セキュリティプログラムを作成する。
(C)情報セキュリティプログラムに沿って、情報セキュリティ対策を実施する。
(D)実際の情報セキュリティ対策の管理・運営が情報セキュリティプログラムに合致するように適宜見直しを行う。

金融機関がこれらの手続きを実行する上で参考になる標準規格や技術報告書として、①ISO/TR 13569（金融業務における情報セキュリティガイドライン）、②ISO/IEC 15408（情報セキュリティ製品・システムの評価基準）、③BS 7799（情報セキュリティ管理ガイドライン）の 3 つが挙げられる。ISO/TR 13569 は、金融機関による情報セキュリティ対策全般の指針を提供する技術報告書であり、ISO/IEC 15408 は、米国やカナダ等 6 か国の統一的な評価基準コモンクライテリア（Common Criteria＜CC＞）に基づいて策定された、情報セキュリティ製品・システムの評価基準に関する国際標準である。また、BS 7799 は、特に情報セキュリティの管理・運用に重点をおいた英国の情報セキュリティガ

イドラインである。

最近では、第三者機関が、ISO/IEC 15408 や BS 7799 に基づいて情報セキュリティの評価・認定を行うための枠組みが整備されつつある。ISO/IEC 15408 に規定されているセキュリティ要件を利用して、金融分野向けのプロテクションプロファイル（Protection Profile＜PP＞）を作成・評価するプロジェクトが進められているほか、本国際標準に基づく評価スキーム（Common Evaluation Methodology＜CEM＞）が検討されている。また、BS 7799 に基づく情報セキュリティ管理・運用体制の評価・認定スキーム c:cure の運用が開始されている（図 1 参照)。

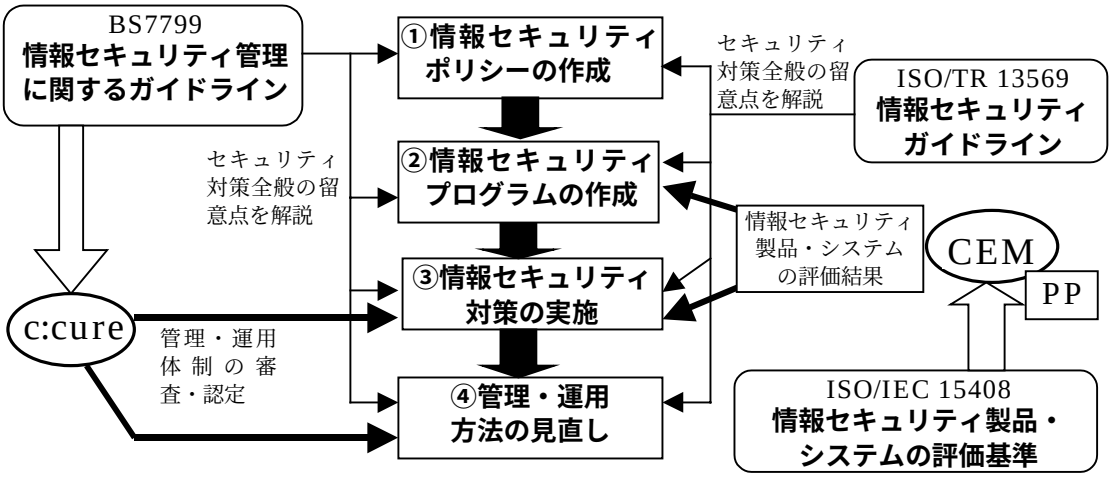


図 1　情報セキュリティ対策の実施手順と関連する標準規格の関係

本稿では、まず第Ⅱ章において、ISO/TR 13569 の概要を紹介した上で、現在進められている改訂内容について説明する。第Ⅲ章では、ISO/IEC 15408 の概要のほか、本国際標準に基づく情報セキュリティ製品・システムの評価スキームとして検討が進められている CEM の概要、金融分野における ISO/IEC 15408 への対応状況について説明する。第Ⅳ章では、BS 7799 の概要を説明するとともに、BS 7799 に基づく情報セキュリティの管理・運用体制に関する評価・認定スキーム c:cure について説明する。

Ⅱ. 金融業務における情報セキュリティガイドライン

1. ISO/TR 13569 の概要

(1)目的

ISO/TR 13569 は、銀行、証券会社等の金融機関が情報セキュリティ対策を実施する際の指針を提供する技術報告書[1]であり、ISO/TC68/SC2[2]において策定された（ISO [1997]）。ISO/TR 13569 策定の目的として、以下の 3 点が挙げられている。

①情報セキュリティプログラムの構造・構成要素について解説する。
②情報セキュリティ対策を講じるための手段を選択する際の指針となる情報を提供する。
③既存の標準規格との整合性だけではなく、策定段階にある標準規格案との整合性もとれた情報セキュリティ対策を実現可能にする。

(2)標準化の経緯

ISO/TR 13569 の第 1 版（ISO[1996]）は 1996 年 11 月に公表されたが、その後、暗号技術の利用に関する記述の追加等が行われ、現在最新版となっている第 2 版が 1997 年 10 月に公表された。

しかし、近年の情報セキュリティ技術の急速な進展や、金融ネットワークのオープン化等の環境変化を背景に、第 2 版の見直しが必要となってきている。このため、ISO/TC68/SC2 では、1998 年 12 月に第 2 版の一部を改訂する「修正第 1 号（Amendment 1）」を発表した（ISO[1998]）。さらに、現在、汎業界向け情報セキュリティガイドライン ISO/IEC TR 13335（GMITS）[3]の内容を取り入れる方針で、第 2 版の全面的な見直し作業が進められている。

---

[1] ISO では、技術進歩のスピードが極めて速い等の理由から、国際標準にはなりにくいものの、公表することによって関連分野において技術を利用する際に有益であると判断された技術情報については、技術報告書（Technical Report＜TR＞）として取り纏められ、公表されている。

[2] ISO/TC68/SC2：ISO/TC68 は、「銀行業務、証券業務およびその他金融サービス」に関する国際標準の策定を担当する専門委員会であり、SC2 は、「セキュリティ管理と一般銀行業務」に関する標準規格の策定を担当する分科委員会である。金融分野における情報セキュリティ技術の国際標準化の体制等については、岩下・谷田部[1999]を参照。

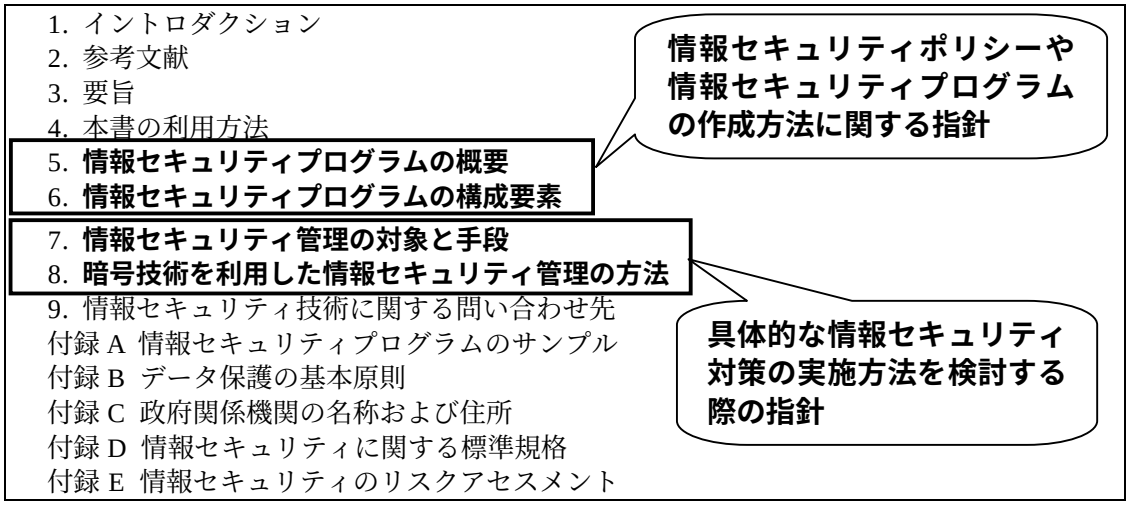
[3] ISO/IEC TR 13335（Guidelines for the Management of IT Security＜GMITS＞）：汎業界向け情報セキュリティ管理の指針を定める技術報告書（ISO/IEC[1997a][1997b][1997c][1997d][1997e]）。GMITS は 5 つの Part から構成されており、Part 1: Concepts and Models for IT Security、Part 2: Managing and Planning IT Security、Part 3: Techniques for the Management of IT Security、Part 4: Selection of Safeguards、Part 5: Management Guideline on Network Security である。

2. ISO/TR 13569 の構成・内容

(1)構成

ISO/TR 13569 第 2 版は、9 つの章と 5 つの付録から構成されており、中心となるのは第 5～8 章である。

ISO/TR 13569 の構成



これらの章は、①情報セキュリティポリシー[4]や情報セキュリティプログラム[5]を作成する際の指針となる第 5 章と第 6 章、②情報セキュリティプログラムを作成した上で、具体的な情報セキュリティ対策の実施方法を検討する際の指針となる第 7 章と第 8 章、の 2 つの部分に大別することができる。

各章には、ISO/TC68 で作成された、または作成中の国際標準が頻繁に引用されている。例えば、暗号技術の実装を検討する際に、金融機関として最低限必要とされる安全性を確保するためにはどの暗号アルゴリズムを利用すべきか、また鍵長の設定や鍵管理等の実装形態をどうすべきかについて、関連する国際標準が明示されている。

(2)情報セキュリティプログラム作成の指針：第 5 章と第 6 章

第 5 章と第 6 章では、情報セキュリティプログラムに盛り込むべき項目が解

---

[4] 情報セキュリティポリシーには内容や具体度に応じて様々なレベルが存在しており、組織の情報セキュリティ対策に関する基本方針を整理した文書を指す場合がある一方、パスワード管理等の具体的な情報セキュリティ手段の利用マニュアル等を指す場合もある。ISO/TR 13569 における情報セキュリティポリシーは、各金融機関の情報セキュリティに対する基本方針を整理した文書に相当する。

[5] 情報セキュリティプログラムは、情報セキュリティポリシーに規定された「セキュリティ対策の基本方針」に基づき、組織として取り組むべきセキュリティ対策の枠組みを規定した文書であり、情報セキュリティ確保に向けた組織管理体制の整備や研修プログラムの策定等、具体的なセキュリティ対策を実施するための指針を提供する。

説されている。まず、①情報セキュリティポリシーの策定が必要であるとされている。その上で、情報セキュリティポリシーに基づいて、②情報セキュリティ管理専門部署の設置方針、③役職員への情報セキュリティに関する研修プログラム、④災害情報等の情報伝達・復旧プラン、⑤情報セキュリティプログラムから逸脱した事象の発見･対応手続き、⑥監査・保険・法務部門との連絡手続き、⑦情報セキュリティプログラムの見直し手続き、⑧監査記録の作成・管理方法、の 8 項目を含む情報セキュリティプログラムの作成が必要である、としている（表 1 参照)。

表 1　情報セキュリティプログラムの主要な構成要素

項目	内容
①情報セキュリティポリシー	情報セキュリティポリシーは、その組織における情報資産の位置付けや管理方法に関する基本方針を規定。
②情報セキュリティ管理専門部署の配置方針	以下の役割を果たす情報セキュリティ管理専門部署を配置。 (A)最新の情報セキュリティ技術や標準化の動向をフォローし、適宜情報セキュリティプログラムに反映。 (B)監査担当者、保険担当者、法務担当者等と適宜意見交換を行い、適切な情報セキュリティプログラムを作成。 (C)情報のリスクに対する意識向上のための啓蒙活動を実施。 (D)情報資産に損害が発生した場合には、その復旧をサポート。
③研修計画	各役職員に情報セキュリティの重要性を認識させ、自分の義務・責任を自覚させるための研修計画を作成。
④情報伝達・復旧プラン	災害発生時に情報資産の損失に伴う業務停止などを回避するために、事前に対応すべき災害の種類・規模を想定し、復旧させるべき業務の優先順位を決定した上で、事前・事後の対応方針を決定。また、情報セキュリティに関連する事故等が発生した場合に、関連部署への情報伝達方法を決定。
⑤情報セキュリティポリシーから逸脱した事象の発見・対応手続き	情報セキュリティ製品やシステムにおいて、情報セキュリティプログラムに規定されている管理方針から逸脱したと考えられる事象を発見し、その原因を明らかにする手順や対応方針を決定。
⑥監査・保険・法務部門との連絡・調整体制	情報セキュリティプログラムの運用は、監査、保険、法務部門と連携を取りながら進めることが必要であるため、調整・連絡体制を整備。
⑦情報セキュリティプログラムの見直し手続き	情報セキュリティ技術の研究動向をフォローし、採用したシステムが十分なセキュリティ水準を確保できているか否かを適宜検証する体制を整備。
⑧監査記録の作成・管理方法	情報資産の管理･運用状況に対して監査を行い、その記録の作成・保管方法を決定。監査人は、監査結果に基づいて情報資産の潜在的なリスクや管理方法について分析を行い、情報セキュリティの担当役員に適切な助言を行う役割を担う。

― 情報セキュリティプログラムを作成する際には、組織の規模、業務内容、リスク許容度等、組織の属性を考慮した上で、リスク分析を実施し、その結果を加味する必要があるとされている。リスク分析の方法は付録 E で説明されている。

(3)具体的な情報セキュリティ対策に関する指針：第 7 章・第 8 章

第 7 章と第 8 章は、具体的な情報セキュリティ製品・システムを管理する際の指針を提供する。内容は、①必要度や機密度による情報の分類、アクセス管理、システム運用記録の管理、システム変更時の管理という 4 つの基本的な管理手段、②コンピューターやネットワーク等具体的な情報セキュリティ製品の管理方法に加え（以上、第 7 章)、③暗号技術を利用する際の指針（第 8 章）である。

①基本的な情報管理手段

基本的な情報管理手段として、(A)情報の分類、(B)論理的なアクセス管理、(C)システム運用記録の管理、(D)システム変更の管理、について解説されている（表 2 参照)。

表 2　4 つの基本的な情報管理手段

項目	内容
①情報の分類	情報を必要度（criticality）と機密度（sensitivity）の 2 つの観点から分類し、分類結果に応じた情報セキュリティ対策を実施。 ― 必要度の観点からは、「不可欠」「重要」「一般」に分類されるほか、機密度の観点からは、「極秘」「機密」「内部限定」「公表可」に分類される。
②論理的アクセス管理	情報の必要度、機密度に応じたアクセス管理を実施。アクセス管理の方法として、利用者 ID とパスワードを用いた方式やバイオメトリックスを利用した方式等を利用する。
③システム運用記録管理	情報の必要度や機密度に応じて、どのようなデータを運用記録として保管するかを決定。運用記録の対象となるデータは、パスワード等による本人確認記録、ファイルの読出／書込作業記録、ネットワークにおける交信記録等が挙げられる。システム管理者は、運用記録を毎日チェックするとともに、運用記録の情報を保管する際には、デジタル署名等を利用して運用記録の完全性を確保。
④システム変更管理	ハードウェア、ソフトウェア、操作マニュアル等あらゆる変更内容に関する記録を保管するとともに、システム変更の申請・承認手続きや新システムの運用テスト実施手続きの整備を実施。

②情報セキュリティ製品・システムの管理方法

具体的な情報セキュリティ製品・システムとして 15 項目が取り上げられており、各製品・システムを管理する際の留意点について説明されている（次頁の表 3 参照)。

表 3　各情報セキュリティ製品の管理方法

	主な管理方法	特に必要度や機密度の高い情報の取扱方法
①コンピューター	電源管理や入退室管理等の物理的保護、論理的アクセス管理、メンテナンス管理、災害発生時における対応、監査記録管理、廃棄管理	**＜極秘・機密情報＞** ・ディスプレイに表示された情報が無権限者に見られないように専用ブースを設置。
②ネットワーク	ダウンしたネットワーク復旧時の対応、アクセス管理、外部ネットワークとの接続管理（ファイアーウォール等）、通信データの保護、設定変更管理、可用性の維持	**＜極秘情報＞** ・情報を暗号化するほか、MAC やデジタル署名を用いて完全性を確保。
③ソフトウェア	データベース管理、システムソフトウェア管理、アプリケーションの運用テスト管理、アプリケーションの誤動作に伴う損失をカバーする手段（保険等）の適用、ソフトウェアの設定変更管理、知的財産権管理、コンピューターウィルス対策、ハードウェアのメモリー管理、リモートアクセス可能なソフトウェアの管理、顧客へのソフトウェアの配送管理	**＜重要・不可欠情報＞** ・資金移動関連情報の取扱には、通常の制御手段が利用不可能になった場合でも対応可能な措置を講じる。 ・MAC やデジタル署名等の機能を有するアプリケーションがウィルス等に感染していないかを確認。 **＜極秘・機密情報＞** ・アプリケーションのテストの際に顧客情報等が外部に漏洩しないような措置（厳重なアクセス管理、既存のシステムとの分離等）を実施。
④人的要因	情報セキュリティの重要性を啓蒙するための研修プログラムの実施、情報管理に関する行動規律の明文化、システムへのアクセス管理等による内部犯罪の防止等	**＜極秘・機密情報＞** ・機密度の高い情報を取扱う部署では、事前通告のない異動を適宜実施。
⑤電話等の音声に関連する製品等	Voice Mail システムへのアクセス管理、PBX システムの管理、口頭での情報伝達時の注意事項、盗聴対策、Voice Response Units の管理	**＜極秘・機密情報＞** ・情報を声に出して伝える場合、周りの人々に注意を払う必要があることを周知徹底する。 ・携帯電話やコードレス電話では、極秘情報をやり取りしない。やり取りする必要がある場合には、暗号化を実施。
⑥FAX	FAX 内容の改ざん・否認対策（デジタル署名の利用）、メッセージの誤送信防止、送信情報の機密管理、Denial of Service 攻撃対策、送受信データの保管・バックアップ	**＜極秘・機密情報＞** ・FAX 番号を間違えないように慎重にダイヤルする。 ・通信データの暗号化を実施。 ・まず表紙を送信し、先方から受信用意が整った旨の連絡が入った後に FAX 送信を開始。
⑦電子メール	メールアカウントへのアクセス管理、メール端末の物理的管理、メール内容の完全性確保、メール内容の機密管理、メール内容の保管・バックアップ、メールの到達確認	**＜極秘・機密情報＞** ・電子メールのタイトルに「機密情報」であることを明示。 ・暗号化を実施。 ・電子メールの宛先が間違っていないかどうかを確認。
⑧紙ベースの書類	内容の改ざん防止、機密管理、文書保管製品の管理、書類廃棄、ラベリング、偽造文書と真正文書の識別、書類のバックアップ	**＜極秘・機密情報＞** ・機密度の高い情報を含む書類等にはラベルを添付し、人目につく場所に置き去りにしない。 ・保管装置には情報セキュリティ対策専門部署が認定したものに限定。 ・廃棄する場合にはシュレッダー等を利用。 **＜重要・不可欠情報＞** ・保管装置には情報セキュリティ対策専門部署が認定したものに限定。
⑨マイクロフィルムや他の記録媒体	機密管理、廃棄管理、バックアンプ管理、保管環境による記録媒体の毀損等の防止	**＜極秘・機密情報＞** ・磁気記録媒体で保管する際には暗号化を実施。 ・マイクロフィルムで保管する場合はラベルを貼付。
⑩金融取引用カード	物理的な保護、個人情報管理、PIN の取扱方法、監査、カードの偽造防止、適切な人事 －　ISO 10202（IC カードを利用した金融取引システムのセキュリティアーキテクチャー）、ISO 9564（PIN の管理とセキュリティ）等の国際標準を参考にして対応。	
⑪ATM	利用者確認、交信情報の完全性確保、機密管理、不正行為の防止、メンテナンス管理 －　鍵配送には、ISO 8732 を参考にして対応。	
⑫電子資金移動	利用者確認、送受信情報の完全性確認、情報の二重使用の防止、関連情報の管理、関連する法律の遵守	**＜重要・不可欠情報＞** ・関連情報の交信には暗号技術を利用したメッセージ認証を実施。
⑬小切手	ANSI X9/TG-2（小切手の様式）、ANSI X9/TG-8（小切手のセキュリティ指針）等を参考にして対応。	
⑭電子商取引	新顧客の身元確認、交信情報の完全性確認	
⑮電子マネー	関連製品の複製・盗難防止、データやソフトウェアの複製・変更防止、データの完全性・否認防止確保	

③暗号技術の利用方法

暗号技術の利用については、(A)暗号化の対象となる情報や暗号の実装形態のほか、(B)メッセージ認証コード（Message Authentication Code＜MAC＞）、(C)デジタル署名、(D)鍵管理、(E)信頼できる第三者機関（Trusted Third Party ＜TTP＞）を利用する際の留意点が解説されている（表 4-1、表 4-2 参照）。

表 4-1　暗号技術の利用方法に関する留意点＜1＞

項目	内容
①暗号化の対象となる情報と実装形態	(a)**暗号化の対象となる情報** 極秘・機密情報が、(i)持ち運び可能な装置に保管される場合、(ii)ネットワークによって送信される場合に、暗号化する。 (b)**守秘目的での暗号の実装方法** 暗号を実装する場合、(i)暗号製品の物理的・論理的なセキュリティをどう評価するか[6]、(ii)どの暗号アルゴリズムを選択するか[7]、等を検討する。
②メッセージ認証コード（MAC）	MAC の生成方法は ISO 8730[8]と 8731[9]に準拠するとともに、MAC に利用する鍵の管理方法に関しては ISO 8732[10]に準拠する。
③デジタル署名	(a)TC68 の標準規格に規定されているデジタル署名方式を利用。 (b)署名生成・検証鍵の生成、管理、配布を TC68 等の標準規格の規定に沿って実行し、紙の文書と同様に、データの機密度等に応じてデジタル署名の生成権限を役職員に割り当てる。 (c)公開鍵証明書を発行する認証機関を選択する場合、その管理・運営状況が ISO/TC68 の国際標準に適合しているか否かを慎重に検討する。

[6] 参考となる標準として NIST の FIPS 140-1*が紹介されている。
*FIPS 140-1：FIPS（Federal Information Processing Standard）は、米国連邦政府内で利用されるコンピューターシステムに関する標準規格であり、NIST によって作成されている。FIPS 140-1 は、Security Requirements for Cryptographic Modules に関する標準規格であり、公開鍵暗号における秘密鍵等を保管する耐タンパー性を有する暗号製品を 4 種類にレベル分けし、各々の要件を定めたもの。

[7] ISO/TC68 の各国際標準に規定されている暗号アルゴリズムを利用するとされている。

[8] ISO 8730 Banking – Requirements for message authentication (wholesale)：銀行のホールセール業務における MAC の利用方法に関する標準規格。MAC のデータフォーマット、生成方法、データ認証手続き、MAC に利用可能なアルゴリズムの認定手続き等が規定されている。なお、現在、ISO/TC68 では、MAC に関する 3 つの国際標準 ISO 8730、ISO 8731（脚注 9 を参照）、ISO 9807（リテール取引に利用されるメッセージ認証の要件）を整理・統合し、ISO/CD 16609（銀行業務に利用されるメッセージ認証の要件）として 1 つの国際標準に置き換えるというプロジェクトが進められている。

[9] ISO 8731 Banking – Approved algorithms for message authentication：ISO 8730 に規定されているアルゴリズム認定手続きに基づいて認定されたアルゴリズムの標準規格。2 つの Part から構成されており、Part 1 には米国政府標準暗号アルゴリズムである DES が規定されているほか、Part 2 には、DES を利用した MAC の生成方法が規定されている。

[10] ISO 8732 Banking – key management (wholesale)：銀行のホールセール業務に利用する暗号の鍵管理に関する標準規格。鍵の生成、配送、保管、廃棄等において安全な鍵管理を実現するための要件が規定されている。

表 4-2　暗号技術の利用方法に関する留意点＜2＞

項目	内容
④鍵管理	(a)**鍵生成** 共通鍵暗号のセッション鍵や公開鍵暗号の公開鍵・秘密鍵を生成する際には、ISO 8732 や ANSI X9.30[11]を参考にする。 (b)**鍵配送** 共通鍵暗号や公開鍵暗号の秘密鍵を配送する場合、ISO 8732 の要件を満足する方法を利用すべき。公開鍵暗号の公開鍵を配送する場合、公開鍵証明書を添付する。 (c)**鍵保管** ISO 8732 の要件を満足する鍵保管方法を採用する。 (d)**公開鍵証明書の管理** 公開鍵証明書廃棄リスト（Certificate Revocation List＜CRL＞）に一定周期でアクセスし、受信した公開鍵証明書の有効性確認を行う。
⑤TTP	TTP は、ある特定の取引において取引当事者や取引内容に対する信頼性を高める機能を有し、暗号鍵の管理、システムへのアクセス管理、公開鍵証明書の発行等、幅広いサービスを提供する第三者機関。TTP を利用する場合、TTP の信頼性を評価した上で、利用するサービスや、万一障害が発生した場合の責任分担等について検討する。 なお、現在 SC27 が TTP の業務内容に関するガイドライン[12]の検討を進めており、この検討結果も参考になる。
⑥災害と暗号技術	暗号技術を利用するシステムにおける災害復興計画（Disaster Recovery Planning＜DRP＞）には、火災や電力障害等への対応方針を規定するとともに、署名生成鍵の漏洩等についても対応方針を規定する。ANSI X9.57[13]には、認証機関における署名生成鍵の漏洩への対応方法が規定されており、これらの標準規格を参考にして検討する。

3. 修正第 1 号の発表

1997 年 10 月に発表された第 2 版は、その後の暗号技術の進歩等によって、内容の一部が陳腐化しつつある。このため、ISO/TC68/SC2 は、1998 年 12 月に修正第 1 号を発表し、第 2 版の一部を改訂した。主な改訂内容は、(1)ア

---

[11] ANSI X9.30 Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry： 金融業務において利用される公開鍵暗号に関する米国標準規格であり、デジタル署名方式として米国連邦政府のデジタル署名標準 DSA が規定されている。

[12] この標準規格案は ISO/IEC PDTR 14516（Guidelines for the use and management of Trusted Third Party）とみられる。本標準案には、TTP サービスとして、タイムスタンプサービス、鍵管理サービス等の内容や業務遂行上の留意点が説明されている。

[13] ANSI X9.57 Public Key Cryptography for the Financial Services Industry: Certificate Management：金融業務で利用される公開鍵暗号システムにおける認証機関や公開鍵証明書の機能や要件が規定されている米国標準規格。なお、現在 ISO/TC68 において標準化が進められている、金融業務で利用する公開鍵証明書の管理、認証機関の機能・要件等を規定する国際標準案 ISO/CD 15782（Banking－Certificate Management）は、ANSI X9.52 に基づいて作成されている。

クセス管理の手段として、公開鍵証明書を用いた方法や盛り込まれたほか、バイオメトリックスを利用する際の留意点が追加されたこと、(2)暗号技術について、共通鍵暗号や公開鍵暗号における推奨最短鍵長が盛り込まれたこと、の 2 点である（表 5 参照)。

表 5　ISO/TR 13569 修正第 1 号の主な内容

改訂点		改訂内容
アクセス管理	公開鍵証明書を用いた認証方式の利用	ユーザーID とパスワードを利用する方式に加えて、認証機関（Certification Authority＜CA＞）が発行した公開鍵証明書によるユーザー認証方式の採用を推奨。公開鍵証明書の管理方法や CA の業務内容等に関する国際標準として、ISO 15782 が挙げられている。 ― 第 2 版のアクセス管理に関する記述は、金融機関の内部端末からシステムにアクセスする際の管理方法の解説が中心であった。本改訂の背景として、修正第 1 号では「金融ネットワークのオープン化の進展に伴い、外部からのアクセスの管理が不可欠」と指摘。
	バイオメトリックスを利用する際の留意点	「バイオメトリックスを利用する場合には、必要なセキュリティ水準やエラー率を勘案しながら、他の本人確認手段と併用して利用する」との記述が追加。 ― 本改訂の理由として、修正第 1 号では、「実際の利用事例におけるエラー率をみると、本人確認手段として単独で採用することは現時点では困難」と指摘。
暗号技術	奨励最短鍵長	共通鍵暗号や公開鍵暗号の推奨最短鍵長が追加。共通鍵暗号の最短鍵長には 80 bit が推奨されており、これと同程度の安全性を有するとみられる楕円曲線暗号の鍵長として 160 bit、その他の公開鍵暗号の鍵長として 1024 bit が推奨されている。
	鍵長選択時の留意点	鍵長を決定する際に考慮すべき項目として、以下の 5 項目が追加。 ①鍵の有効時間（どの程度の頻度で鍵を変更するか） ②鍵の再利用回数（1 つの鍵をどの程度の頻度で再利用するか） ③暗号技術による保護の対象となる資産の価値と、暗号化されている時間 ④必要とされる処理速度 ⑤暗号以外のセキュリティ対策の有無 さらに、金融機関は暗号方式を選択する場合、ISO の国際標準や各国内標準を参考にするとしている。

4. ISO/TR 13569 第 3 版に向けた改訂作業

現在 TC68/SC2 は、修正第 1 号の発表に続き、GMITS（脚注 3 参照）の内容を取り入れることを主な目的として、ISO/TR 13569 の見直し作業を進めている。1999 年 8 月 19 日時点の草案は 12 の章から構成されている（図 2 参照）。

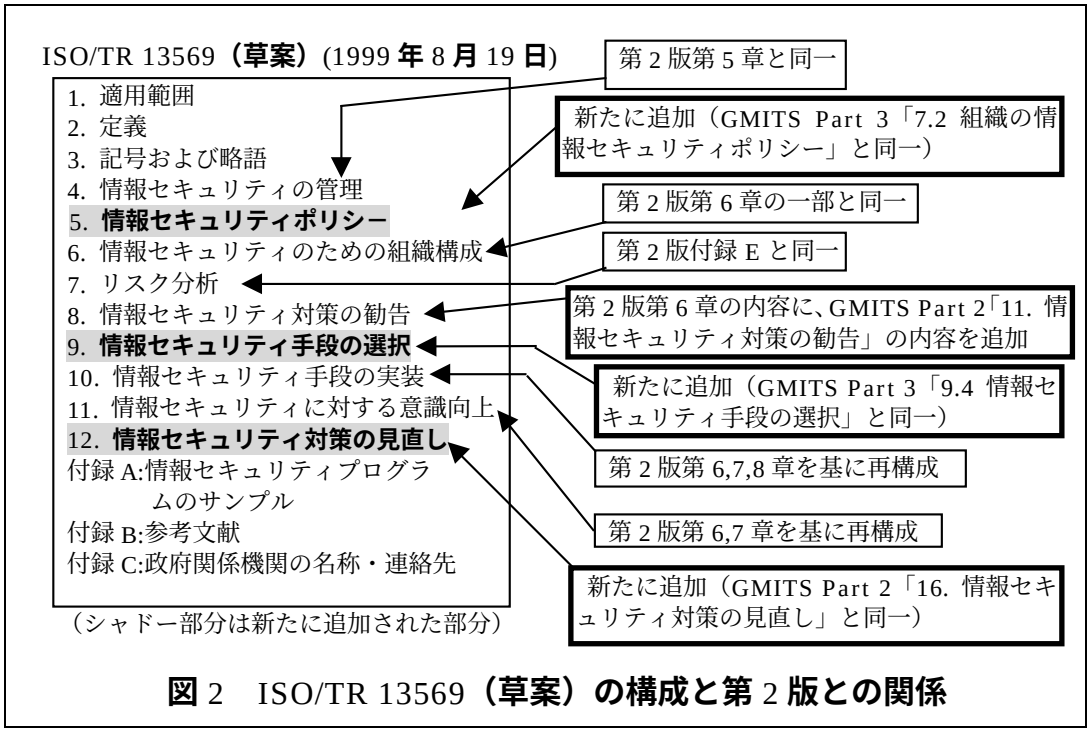


図 2　ISO/TR 13569（草案）の構成と第 2 版との関係

新たに追加された部分等、主な変更点は以下の 6 つ。

①GMITS Part 3「7.2 組織の情報セキュリティポリシー」の内容を「第 5 章：情報セキュリティポリシー」として追加。
②第 2 版「第 6 章：情報セキュリティプログラムの構成要素」に GMITS Part 2「11. 情報セキュリティ対策の勧告」の内容を加えて、「第 8 章：情報セキュリティ対策の勧告」として編成。
③GMITS Part 3「9.4 情報セキュリティ手段の選択」の内容を「第 9 章：情報セキュリティ手段の選択」として追加。
④第 2 版の第 6、7、8 章の内容を基に「第 10 章：情報セキュリティ手段の実装」として編成。
⑤第 2 版の「6.7 情報セキュリティに対する意識向上」と「7.8 人的要因」の内容を基に「第 11 章：セキュリティに対する意識向上」として編成。
⑥GMITS Part 2「16. 情報セキュリティ対策の見直し」の内容を「第 12 章：情報セキュリティ対策の見直し」として追加。

こうした章構成により、情報セキュリティ対策の検討手順、すなわち、「情報セキュリティポリシーの作成」→「情報セキュリティプログラムの作成および管理体制の整備」→「リスク分析」→「情報セキュリティ手段の選択と

実装」→「セキュリティ対策の見直し」というプロセスが明確となっている（図 3 参照）。

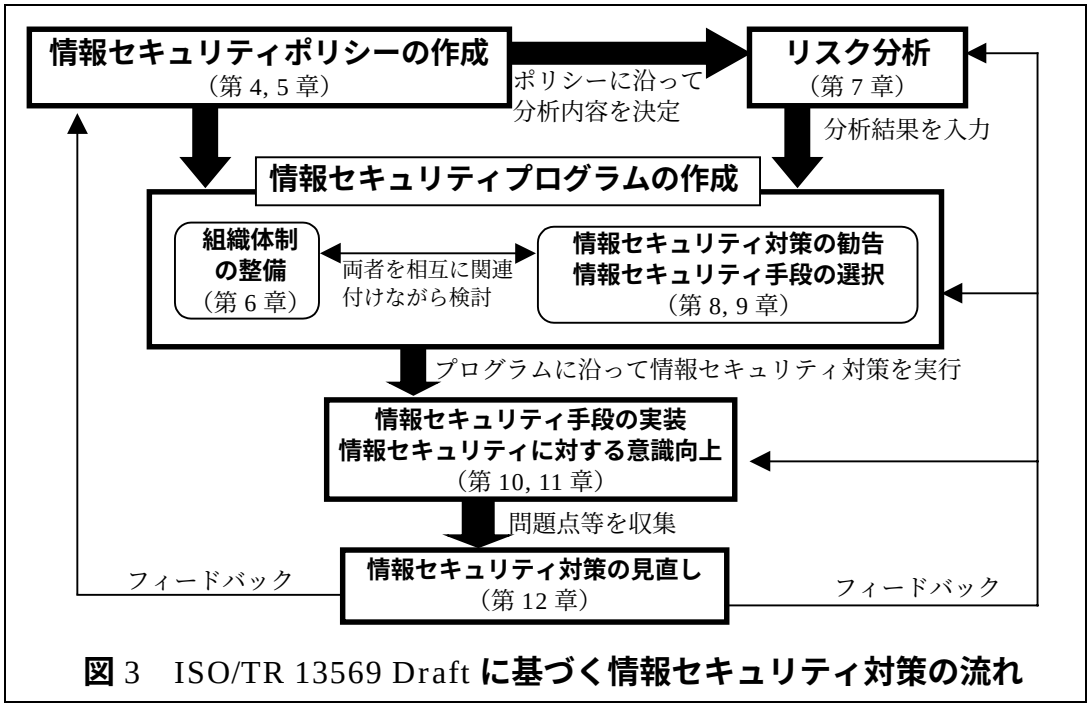


図 3　ISO/TR 13569 Draft **に基づく情報セキュリティ対策の流れ**

(1)第 5 章：情報セキュリティポリシー

第 2 版では、情報セキュリティーポリシーの概要とサンプルがそれぞれ第 5 章と付録 A に記載されているのみであった。これに対し、草案では、GMITS Part 3「7.2 組織の情報セキュリティポリシー」の内容がそのまま第 5 章として採用され、情報セキュリティポリシーの重要性や規定すべき 19 の項目が詳しく説明されている。内容は、以下の 3 点に集約することができる。

①情報セキュリティポリシーは、組織の目的、特徴、経営方針を十分反映した内容とする。
②情報セキュリティポリシーを策定する際には、監査、財務、情報システム、設備、人事、セキュリティ、経営管理を担当する役員が参画し、最終的には最高経営責任者が承認する。
③情報セキュリティポリシーの内容を各役職員に周知し、情報セキュリティに対する責務を自覚させるための研修等を実施する。

(2)第 8 章：情報セキュリティ対策の勧告

本章では、第 7 章に解説されているリスク分析の結果を受けて、情報セキュリティ対策の必要性を勧告するために、①組織のリスク許容度、②必要となる情報セキュリティ手段の候補、②情報セキュリティ対策によって得られる便益と残されるリスクについて分析すべきであると説明されている。本章の

内容は、GMITS Part 2「11. 情報セキュリティ対策の勧告」と第 2 版「6.2 リスクの受容」から構成されている。

(3)第 9 章：情報セキュリティ手段の選択

本章は、第 8 章の情報セキュリティ対策に関する勧告において、情報セキュリティ手段を選択する際の手順を説明するものであり、GMITS Part 3「9.4 情報セキュリティ手段の選択」の内容がそのまま採用されている。情報セキュリティ手段を選択する際の手順を整理すると、以下の通り。

①既存もしくは計画中の情報セキュリティ手段が存在する場合、その機能や特徴を分析する。
②リスク分析の結果を基に候補となる情報セキュリティ手段をリストアップし、費用面から比較を行う。
③上記②のプロセスにおいて情報セキュリティ手段を絞り込んだ上で、利便性、操作の容易性、利用者へのサポート体制、付加機能のタイプ等を考慮しつつ、さらに絞り込みを行う。
④絞り込まれた情報セキュリティ手段において、システムの個別のセキュリティ要件が満足されると同時に、システム全体のセキュリティが確保されているか否かを確認する。

(4)第 10 章：情報セキュリティ手段の実装

第 10 章は第 2 版の第 6〜8 章によって構成されている。主要な変更点は、「10.19 その他」から 2000 年問題に関する記述が削除された点である。

(5)第 11 章：情報セキュリティに対する意識向上

本章は、第 2 版「6.7 情報セキュリティに対する意識向上」と「7.8 人的要因」の内容を併せたものである。各役職員の情報セキュリティに対する意識を高めるための研修プログラムの必要性や、人的要因によって発生する情報セキュリティに対するリスクの種類と対応方法について説明されている。

(6)第 12 章：情報セキュリティ対策の見直し

本章の内容は、GMITS Part 2「16. 情報セキュリティ対策の見直し」と同一であり、一旦構築したシステムが適正に運営・管理されているか、また、情報セキュリティプログラムやシステムの見直しが必要かを適宜検証するための体制整備が重要であると説明されている。具体的には、①セキュリティ手段のメンテナンス、②情報セキュリティポリシーで要求されるセキュリティ水準が確保されているか否かの検証、③運用環境の監視、④ログ記録の管理、⑤誤動作等の事故への対応方法について説明されている。

Ⅲ. 情報セキュリティ製品・システムの評価

1. セキュリティ基準・評価に関連した国内の動き

国内におけるシステムや製品の安全対策基準としては、1977 年に通産省が策定した「電子計算機システムの安全対策基準」や 1987 年に郵政省や自治省が策定した「情報通信ネットワーク安全・信頼性基準」などが挙げられる（表 6 参照)。その後、通産省や警察庁等において、各種検討委員会における検討結果を踏まえ、それまでに策定されていた各種基準の改定作業が進められてきた。しかし、現在に至るまで国内に統一的な評価基準というものは完成していない。

表 6　セキュリティに関する行政の取り組み

	ガイドライン	各種委員会報告書	システム監査
通産省	・「電子計算機システムの安全対策基準」（1977 年） ・「情報システム安全対策基準」（1995 年 8 月：通産省告示 518 号）	・「セキュリティ・プライバシ関連施策の展開について」（1995 年 7 月：セキュリティ・プライバシ問題検討委員会報告書）	・「システム監査基準」（1996 年 1 月：通産省広報）
警察庁	・「情報システム安全対策指針」（1997 年 9 月：国家公安委員会告示）	・「情報システムの安全対策に関する中間報告」（1996 年 4 月：情報システム安全対策研究会） ・「情報セキュリティ調査研究報告書」（1997 年 4 月：情報セキュリティ調査研究委員会）	――
その他	・「情報通信ネットワーク安全・信頼性基準」（1987 年：郵政省、自治省） ・「金融機関等コンピュータシステムの安全対策基準」（1998 年：（財）金融情報システムセンター）	――	――

一方、社団法人日本電子工業振興協会は、コンピューターシステムのセキュリティ要件を整理した「コンピュータセキュリティ基本要件（機能編・保証編)・第 2 版」を 1997 年 8 月に発表した。また、1998 年 12 月には、情報処理振興事業協会が、1999 年に ISO の標準規格となった情報セキュリティ評価基準 CC の一部を和訳し、「CC セキュリティ要件概説書」を発表している。

2. セキュリティ基準・評価に関連した国外の動き

～ISO/IEC 15408 策定に至る背景と現状～

従来から、欧米各国では、政府機関がセキュリティ関連製品を調達する際のベンチマークとして情報セキュリティ評価基準を策定してきた。米国では、国防機関において利用されるセキュリティ関連製品の評価基準として TCSEC（Trusted Computer Security Evaluation Criteria、通称オレンジブック）が 1985 年に策定されており、国防総省の下部機関である NCSC（National Computer Security Center）が、TCSEC に基づいて情報セキュリティ関連製

品の評価・認定を行っている[14]。また、欧州では、欧州委員会が、政府部門に加えて民間部門での利用も視野に入れた情報セキュリティ関連製品・システムの評価基準 ITSEC（Information Technology Security Evaluation Criteria）Ver. 1.2 を 1991 年に発表している。ITSEC は、TCSEC のほか、英国、ドイツ、フランスにおける政府機関向け情報セキュリティ関連製品の評価基準を参考にして策定されたといわれており（菅[1992]）、1993 年には ITSEC に基づく情報セキュリティ製品の評価・認定スキーム ITSEM（IT Security Evaluation Manual）が策定されている[15]。カナダにおいても、TCSEC および ITSEC を参照して、1993 年に政府機関向けの情報セキュリティ関連製品の評価基準 CTCPEC（Canadian Trusted Computer Product Evaluation Criteria）Ver. 3.0 を策定している（表 7 参照）。

表 7　欧米における情報セキュリティ製品・システムの評価基準

国・地域	評価基準	対象分野	公表年	評価機関
米国	TCSEC	国防機関	1985 年	NCSC
欧州	ITSEC	政府機関および民間	1991 年	英国の CLEFs 等、各国の認可機関によって認可を受けた機関
カナダ	CTCPEC	政府機関	1993 年	SCC[16]から認可を受けた機関

[14] NIST*と NSA**は、1993 年、国防関連機関以外の政府機関が利用する情報セキュリティ製品のセキュリティ機能・保証要件を整理した FC（Federal Criteria for Information Technology Security）を策定している。

*NIST（National Institute for Standards and Technology）：米国内における科学技術全般の標準化や、米国政府内で利用される技術の標準化を担当する商務省の下部組織。

**NSA（National Security Agency）：国家安全保障の観点から米国内外で通信情報の諜報活動を行う国防総省の下部組織。暗号技術についても高度な技術力を有しており、NIST の情報セキュリティ技術の標準化活動に対して助言を行っている。

[15] 英国、フランス、ドイツの 3 か国間では、ITSEC および ITSEM に基づく情報セキュリティ製品・システムの評価・認定について相互承認協定（Mutual Recognition Agreement ＜MRA＞）が結ばれており、各国の評価機関によって発行された認定書が他の 2 国においても有効なものとして認められている。評価・認定の枠組みに関しては、例えば英国の場合、政府機関における情報セキュリティ製品の調達基準の策定等を担当している CESG（Communications Electronics Security Group）と貿易産業省（Department of Trade and Industry＜DTI＞）の下で認可機関 UKAS（United Kingdom Accreditation Service）が運営されており、UKAS から認可を受けた評価機関 CLEFs（Commercial Evaluation Facilities、評価機関の総称）が ITSEC、ITSEM に基づく情報セキュリティ関連製品・システムの評価・認定を行っている。現在、英国には 5 つの CLEFs が存在している（詳細については、http://www.ukas.com/および http://www. itsec. gov.uk/info/を参照）。

[16] SCC（Standards Council of Canada）：カナダにおける各種評価機関の認可プログラム PALCAN（The Program for the Accreditation of Laboratories – Canada）に基づいて様々な分野における評価機関の認可を行う認可機関。PALCAN や SCC の詳細については、http://www.scc.ca/palcan/index.html を参照。

このように、欧米では、各国・各地域において独自の評価基準が策定されてきた。しかし、各評価基準やその運用方法は区々であり、国際的な相互運用性に欠けるとの問題点が指摘されていた。このため、米国、カナダ、英国、フランス、ドイツの 5 か国は、1994 年に CCEB（Common Criteria Editorial Board）と呼ばれる協議会を組成し、既存の各評価基準を統一し、その成果を ISO の国際標準にすることを目的とする「CC プロジェクト」を開始した。

CCEB は、1996 年 1 月に CC Ver. 1.0 を完成した後、同年 4 月に ISO/IEC JTC1/SC27/WG3 に提案し、CD（Committee Draft）として承認された。その後、CCEB は、オランダを加えて CCIB（Common Criteria Implementation Board）と名称変更し[17]、1998 年 5 月に CC Ver. 2.0 を発表した。CC Ver. 2.0 には若干の変更が加えられ、1999 年 6 月、情報セキュリティ関連製品・システムの評価基準の国際標準 ISO/IEC 15408（ISO/IEC[1999a][1999b][1999c]）として成立した。また、ISO/IEC 15408 として国際標化された CC Ver. 2.0 の改訂版は、1999 年 10 月に CC Ver. 2.1 として発表された（表 8 参照）[18]。

表 8　ISO/IEC 15408 策定の経緯

時期	米国	欧州（英国、ドイツ、フランス、オランダ）	カナダ
1985 年	TCSEC の策定		
1991 年		ITSEC の策定	
1993 年			CTCPEC の策定
1994 年	CCEB の発足、CC プロジェクトの開始		
1996 年	CC Ver. 1.0 の完成、SC27/WG3 への提案（CD として承認）		
1998 年	CC Ver. 2.0 の完成		
1999 年	ISO/IEC 15408（CC Ver. 2.0 の改訂版）の成立、CC Ver. 2.1 の発表		

3. CC とは

(1)位置づけ

CC は、個々の情報セキュリティ関連製品・システムが備えるセキュリティ機能および品質を統一化された評価尺度に基いて第三者機関が客観的に評価・認定する際に用いられる評価基準の国際標準である。利用者は、評価を受けた製品・システムのセキュリティ水準が必要なレベルに達しているか、またその製品・システムを利用した場合にはセキュリティ・リスクをどの程度考慮する必要があるかを判断する目安として利用することができる。

---

[17] CCIB は、1998 年央に、CC Ver. 2.0 を管理する組織 CCIMB（Common Criteria Interpretation Management Board）として再び名称変更されている。

[18] CC Ver. 2.1 は http://csrc.nist.gov/cc/ccv20/ccv2list.htm から入手可能。

CC における評価の対象には、ハードウェア、ソフトウェアパッケージだけではなく、ある業務を実行するためのアプリケーションシステム全体も含まれる。こうした評価対象は、予め目標として設定されたセキュリティレベルを満たすように設計・開発されると考えられることから、CC では、そうした場合に必要となるセキュリティ機能要件や保証要件が網羅的に列挙されている。製品の利用者、開発者、評価者は、CC の記載内容を元にセキュリティ要件書やセキュリティ設計基本書等を作成した上で、製品の設計・開発・評価を行うこととなる。

CC に基づいて評価された内容（認定された品質保証レベル）は、CC の評価結果に関する MRA が締結された国々において有効な評価として扱われることになる。現在、米国、英国、ドイツ、フランス、カナダ、オランダが相互認証協定と締結している。CC に基づく評価を行う機関は、各国間での合意の下に、中立的な機関として運営されることになると考えられる。

まず、CC の説明において頻繁に使われる用語・略語を整理すると、以下の表 9 の通り。

表 9　CC で用いられる用語の説明

正式名称	略語	内容
Evaluation Assurance Level	EAL	CC に規定されているセキュリティ保証要件の満足度に応じて決定されるセキュリティ保証レベル
Protection Profile	PP	CC の評価対象となる製品・システムを特定の分野に適用する場合に必要となるセキュリティ要件を整理した文書
Security Target	ST	PP の要件に基づいて作成された製品やシステムのセキュリティに関する設計基本書
Target of Evaluation	TOE	CC の評価対象となる情報システム、または情報システムを構成する個々の製品

(2)想定される関連組織と役割

現時点では、CC に基づいたセキュリティ評価の実現方法は国毎に区々である。CC で規定されている手続きや既存の欧米における評価制度から想定されるセキュリティ評価のための組織や役割は以下の通り（図 4 参照）

①評価・監督機関

- **認可機関（Accreditation Authority）**

  認可機関は、CC に沿ったセキュリティ評価を行う機関や、その評価結果の正当性を認証する機関等を認可する機関である。国際間の評価結果の相互承認を責任あるものにするために、国家もしくはそれに準ずる機

関により運営されることになると考えられる[19]。

・**評価機関（Evaluation Facility）**

評価機関は、CC に定められた情報に基づき、情報セキュリティ関連製品・システムを評価する機関であり、認可機関によって認可される。評価機関は、評価結果をまとめた報告書を作成する。評価機関の運営主体は、公的機関のほか民間機関の場合も考えられる。

・**認証機関（Certification Authority）**

認証機関は、評価機関が行った評価が正当であることを検証し、正当であると判断した場合には認証書を発行する機関である。評価結果は、認証書とともに、カタログに登録される。

②情報セキュリティ関連製品・システムの利用者

情報セキュリティ関連製品・システムの利用者（業界団体等）は、利用する製品・システムに必要とされるセキュリティ要件を整理した PP を定める。PP の内容は、CC に規定されているセキュリティ機能要件（CC の Part 2 に規定）とセキュリティ保証要件（CC の Part 3 に規定）から選択して構成することが推奨される。

利用者は、実際に自社のシステムを構築する際に、評価機関および認証機関による評価結果（認証機関が管理するカタログから参照）を参考にして製品・システムを選択する。

③情報セキュリティ関連製品・システムの設計・開発者

情報セキュリティ関連製品・システムの設計・開発者は、利用者が定めた PP を参考にしながら、各製品のセキュリティ仕様の基となるセキュリティターゲット（Security Target＜ST＞）を定める。ST の内容は、CC に規定されているセキュリティ機能要件とセキュリティ保証要件から選択して構成することが推奨される。

設計・開発者は、作成された ST に準拠して各製品を製造する。製品のセキュリティレベルに関する評価を希望する場合には、準拠した ST と共に評

[19] 例えば、米国では、1997 年に CC に基づく評価制度 NIAP（National Information Assurance Partnership）を発表し、NIST が認可機関となっているほか、評価機関および認証機関としてそれぞれ CCTLs（Common Criteria Testing Laboratories、民間の評価機関の総称）、NVLAP（NIAP Validation Body）が存在する。また、英国においても、CC に基づく評価制度が整備されつつあり、認可機関および認定機関としてそれぞれ UKAS、CESGが担当する方向で検討されている。詳細については、IPAのホームページ（http://www.ipa.go.jp/SECURITY/ccj/ninshou/seido.html）を参照。

価機関に評価を依頼する。

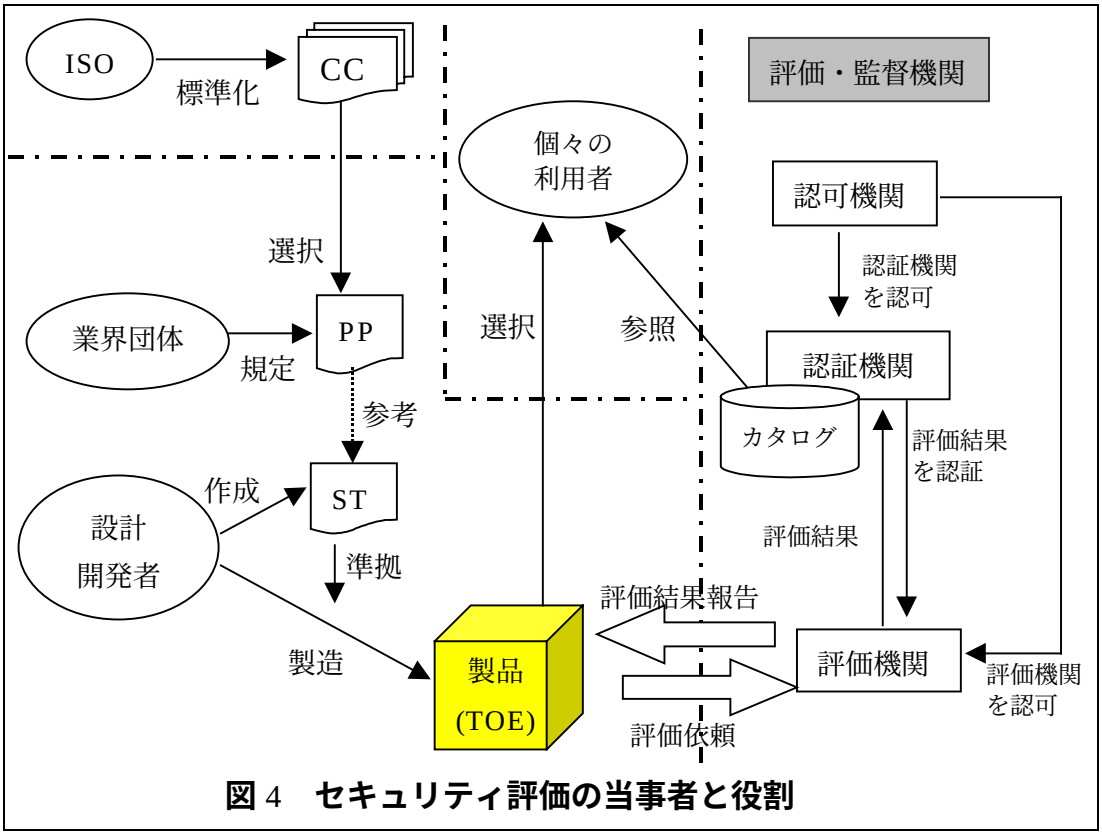


図 4　セキュリティ評価の当事者と役割

(3)**評価の手順**

情報セキュリティ関連製品・システムの評価についても、CC の内容や既存の欧米の制度から、以下の手順が想定される（図 4 参照)。

①利用者（または業界団体）は、IC カードやファイアーウォール等、評価対象のカテゴリーごとに必要とされるセキュリティ機能要件と保証要件を CC の評価モデルを参考にして選択し、PP を作成する（CC の付録 B に PP の概要が記載されている)。

②設計･開発者は、適用分野の PP を参考にして、個々の製品･システム（TOE）の ST を作成する（CC の付録 C に ST の概要が記載されている)。さらに、ST に基づいて TOE を製造する。

③評価機関は、ST に基づいて開発・製造された TOE のセキュリティ水準を、基となった PP および ST とともに、予め規定された手続きに沿って評価する。なお、TOE の実装環境（運用や管理体制等）も評価対象に含まれる。評価は、次のような観点から行われる。

・TOE が必要な（ST に記載されている）セキュリティレベルを備えて

いるか。
・TOE がその利用環境で想定される脅威に対処できているか。
・外部から不正な干渉を受けないような構成になっているか。
・セキュリティ上好ましくない処理を含んでいないか。
・過去に発見されたセキュリティ上の問題が解決されているか。

評価方法の詳細については、現在 CEM として検討が進められている（詳細は本章 5.を参照）。

④認証機関は、評価機関による評価が正当に行われたか否かを検証し、評価が正当なものであると判断した場合には認証書を発行する。評価結果と認証書は、認証機関が管理するカタログに登録される。

⑤個々の情報セキュリティ製品・システムの利用者は、適宜認証機関のカタログを参照することができる。

4. CC の構成と概要

CC は、Part 1（概要と一般モデル）、Part 2（セキュリティ機能要件）、Part 3（セキュリティ保証要件）の 3 つの Part から構成されている。各 Part の概要は以下の通り。

(1)Part 1: 概要と一般モデル

CC に基づいてセキュリティ製品やシステムを評価する場合、その製品・システムを評価するための評価モデルに当てはめる必要がある。Part 1 では、CC において利用される用語や概念を整理するとともに、CC におけるセキュリティ評価の土台となる一般モデルの概要について説明している。一般モデルを構成する要素としては、①TOE、②利用者、③セキュリティに対する潜在的脅威（無権限者による情報の傍受、改変、破壊等）、④対策、⑤対策では十分にカバーできないリスク、等が列挙されている。また、TOE の評価に必要な PP や ST の概要やその利用方法が説明されている。

(2)Part 2: セキュリティ機能要件

Part 2 では、TOE のセキュリティ機能要件について説明されている。セキュリティ機能要件は TOE に必要とされるセキュリティ機能を規定するものであり、11 の要件によって構成されている。各項目は、①クラス、②ファミリー、③コンポーネントの 3 層構造となっており、機能要件の内容が細かく規定されている。セキュリティ機能要件の内容は以下の表 10 の通り。

表 10　セキュリティ機能要件

項番	機能要件（クラス）	内容
1	識別と認証	利用者を特定する必要がある場合に前提となる要件
2	評価対象へのアクセス	不正利用を防止するための要件
3	利用者データの保護	アクセス管理による利用者データ保護のための要件
4	資源利用	利用者妨害を排し、サービスの提供を維持するための要件
5	信頼できる通信路	評価対象と利用者間で安全な通信経路を確保するための要件
6	セキュリティ機構の保護	セキュリティ機構の正常な動作を確保するための要件
7	セキュリティ通信	送受信データの真正性確保や否認防止を実現するための要件
8	プライバシー	匿名性の確保や利用者個有情報の転用防止に関する要件
9	暗号鍵管理	暗号鍵の生成、配送、廃棄やデジタル署名利用に関する要件
10	セキュリティ監査	動作記録や保護すべきデータの利用記録の管理に関する要件
11	セキュリティ管理	セキュリティ機能の安全な運用・管理を実現するための要件

(3)Part 3: **セキュリティ保証要件**

Part 3 では、TOE のセキュリティ保証要件とその評価レベル EAL について説明されている。セキュリティ保証要件は、各セキュリティ機能がどの程度確実に実現されているのかを評価するための要件であり、10 の要件から構成されている（表 11 参照)。各保証要件は、セキュリティ機能要件と同様に、①クラス、②ファミリー、③コンポーネントという 3 つの階層によって構成されている。

表 11 セキュリティ保証要件

項番	保証要件(クラス)	内容
1	PP 評価	PP に記載されるべき項目に関する要件。
2	ST 評価	ST に記載されるべき項目に関する要件。
3	構成管理	構成管理（評価対象の開発・製造工程における一貫性を確保するための管理方法）に関する要件。作業工程の一ヵ所で変更が発生した際の対応方針等について規定されている。
4	配送とその運用	開発先から利用者への評価対象の配送に関する要件。評価対象を安全に配送するための方法や手続きが規定されている。
5	開発	評価対象の開発・製造工程に関する要件。評価対象の機能要件の設定方法、設計書、各開発工程における作業内容等について規定されている。
6	解説書	利用者やシステム管理者に配布される利用・運用解説書に関する要件。解説書の理解しやすさや完成度について規定されている。
7	ライフサイクルサポート	評価対象のライフサイクルに応じたサービスに関する要件。障害対策手順や利用者からのクレームへの対応方法等について規定されている。
8	テスト	評価対象のセキュリティ機能が ST で規定された要件を満足しているか否かを確認するテストに関する要件
9	脆弱性分析	運用環境上想定される脆弱性や誤動作等への対応策に関する要件
10	メンテナンス	評価対象のメンテナンスに関する要件。メンテナンス計画、メンテナンス実施履歴、セキュリティ機能の安全性レベル等が規定されている。

EAL は、評価対象のセキュリティ保証要件に関する保証レベルを表すものであり、7 項目のセキュリティ保証要件（構成管理、配送とその運用、開発、解説書、ライフサイクルサポート、テスト、脆弱性分析）の満足度に応じて決定される。EAL は 7 段階（EAL 1 から EAL 7）となっており、EAL 1 から EAL 7 になるほどの品質の保証レベルが向上する。一般的に利用される商用のセキュリティ製品やシステムは、EAL 3 ないしは EAL 4 のレベルとされている。

(4)PP と ST

①CC、PP、ST の関係

CC、PP、ST は、セキュリティ評価を行う上で、その内容において一定の関係が存在する（図 4 参照）。また、PP と ST は、その適用領域やサービス内容によって、多くのバリエーションが派生しうる（図 5 参照）。

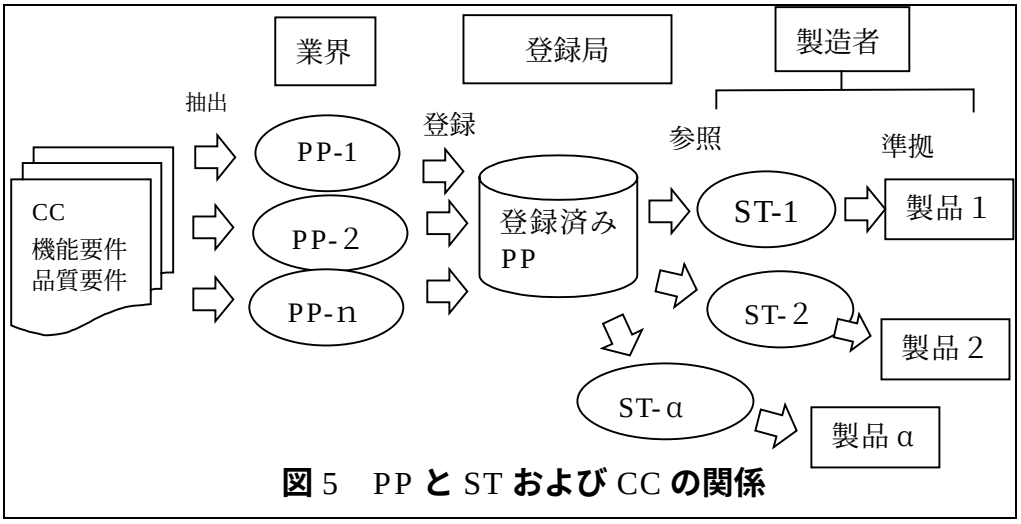


図 5　PP と ST および CC の関係

PP は、その適用領域が類似した業界ごとに定められると考えられるが（例えば、金融システム向け IC カード用 PP）、１つの業界内で複数の PP が存在することもあり得る。また、PP の作成・登録は、個人・法人・組織のいずれもが可能である。PP は、公的機関として運用される登録局（Registration Authority＜RA＞）に登録されることにより公知になり、評価機関が評価を行う際の参考情報となる。登録された PP は再利用されることを前提としており、主として ST や他の PP を作成する場合の参考情報として用いられる。ただし、登録された PP をそのまま利用（結合）して新たな PP を作ることは、著作権上の配慮から禁止されている。PP の内容は以下の表 12 の通り。

表 12　PP の内容

項目			内容
概要	PP の識別		PP を識別するための情報（PP 名、著者、評価状況、EAL レベル）を記述する。
	PP の概要		対象とする読者やこの PP により解決できる問題を記述し、PP の全体を分かり易く記述する。
	関連 PP と参考文献		関係する PP について差分を中心にを記述。適用分野に関して脅威分析や環境を理解する上で整理されている文書があれば記載する。
	PP の構成（ｵﾌﾟｼｮﾝ）		読者に PP を読み易くするために構成を記述する。
TOE 記述			PP が想定する製品を理解するために参考となる情報（TOE が持つ機能、使われ方、操作環境など）や製品のタイプを記述する。
TOE セキュリティ環境			TOE が利用される環境のセキュリティ面の条件について記述する。
	前提条件		TOE の想定する使い方や、走行環境についての物理的な防御手段、外部との接続状態などを記述する。
	想定される脅威		TOE のセキュリティが想定する脅威について、脅威となるエンティティ、守る資源、攻撃方法などについて記述する。
	組織的なセキュリティ方針		TOE を管理・運用する組織のセキュリティ方針を記述する。製品やシステムの保護対象資源の利用方針を規定する。
セキュリティ目標	TOE に関するセキュリティ目標		技術的に対処可能なセキュリティ目標を記述する。
	環境に関するセキュリティ目標		技術的に対処できない脅威に対処するための運用規則や物理的対策を記載する。
IT セキュリティ要件	TOE セキュリティ要件	機能要件	CC Part2 から抽出して記述する。適当な用件が無ければ開発者自身が独自の機能要件を定義してもよい。
		保証要件	CC Part３から必要な EAL を選択して記述する。
	IT 環境のためのセキュリティ要件		TOE が機能する環境の要件を記述する。
PP アプリケーションノート（ｵﾌﾟｼｮﾝ）			TOE の構築・使用・評価に関して有用と考えられる追加補助情報を記述する。
根拠	セキュリティ目標根拠		想定される脅威や保護すべき資源の利用規則に対してセキュリティ方針が適合しているか否かを検証でき、適合していることを示す根拠を記述する。
	セキュリティ要件根拠		セキュリティ要件の選択を正当化するとともに、記載した機能や品質保証要件が想定した脅威や品質保証レベルが低すぎないことの根拠を記述する。

ST は、主たる対象となる利用者に適したセキュリティレベルを達成するための仕様として作成され、評価機関が評価を行うときの参考情報として用いられる。設計・開発者は、対象とする分野の利用者（業界団体）が作成した PP を参考にして ST を作成する。そのため、設計・開発者毎に異なる ST が作成されることとなる。また、PP が存在しない場合には、他の業界の PP を参考に ST を作成することが必要となる。ST の内容は以下の表 13 の通り。

表 13　ST の内容

項目		内容
ST イントロダクション	ST 識別	ST を識別するための名称等を記述する。
	ST 概要	ST の概要を記述する。
	CC 適合	CC の適合性について記述する。
TOE 記述		ST に記されているセキュリティ要件を理解するために参考となる情報や製品のタイプを記述する。
TOE セキュリティ環境		TOE が利用される環境のセキュリティ面の条件について記述する。前提条件、想定される脅威、組織的なセキュリティ方針について記述する。
セキュリティ目標		TOE に関するセキュリティ目標、環境に関するセキュリティ目標について記述する。
IT セキュリティ要件		TOE セキュリティ機能・保証要件、IT 環境のセキュリティ要件、について記述する。
TOE 要約仕様	TOE セキュリティ概要	機能要件を満たすことを検証するために製品などが提供する具体的な機能仕様を規定する。特別なセキュリティ機能を組み込む場合には機能仕様との対応を記述する。
	保証対策	保証レベルを満たすための開発手法を記述する。具体的には、製品開発管理、処理の無矛盾性、運用状況への考慮、潜在的脅威への対処等を記述する。
PP 宣言		既存 PP の要件の採用具合を記述する。その場合追加や修正も可能である。
根拠	セキュリティ目標根拠	想定される脅威や保護すべき資源の利用規則に対してセキュリティ方針が適合しているか否かを検証でき、適合していることを示す根拠を記述する。
	セキュリティ要件根拠	セキュリティ要件の選択を正当化するとともに、記載した機能や品質保証要件が想定した脅威や品質保証レベルが低すぎないことの根拠を記述する。
	TOE 要約仕様根拠	上記「TOE 要約仕様」に記述された機能・対策が TOE セキュリティ要件を満たす根拠を記述する。
	PP 宣言根拠	ST が適合しているとする PP との相違やセキュリティ目標とセキュリティ要件の相違について記述する。ある特定の PP に準拠性を宣言することにより記述を省略することができる。

②PP と ST の作成・登録に関する動向

(A)米国における CS2 の作成

CC に基づく PP については、既にファイアーウォール、データベース、IC カード等に関する PP が欧米諸国において作成されつつある。こうした動きを促進するために、NIST は、一般的な商用レベルの製品・システムの PP を作成する際の手引書として、CS2（Commercial Security 2）の作成を進めており、1998 年 12 月には CS2 Ver. 0.4 を発表している（NIST[1998]）[20]。

[20] 日本電子工業振興協会コンピュータセキュリティ評価基準専門委員会では、1997 年 8

CS2 において想定されている製品・システムは、CC におけるセキュリティ保証レベルで EAL2 を満たすものとされている。具体的には、スタンドアローンまたは分散型マルチユーザー情報システムが想定されており、それらのシステムへのアクセス形態として、①一般に公開されたウェブサイト上の情報へのアクセス等、利用者がユニークな識別情報を予め付与されていない形態でのアクセスと、②利用者がユニークな識別情報を予め付与され、システムへのアクセスを行うのに先立って利用者の認証が行われる形態のアクセスが前提とされている。また、システムへアクセスする利用者すべてが、悪意をもたず、システムへの不正侵入を実行するための高度な能力を有しない環境が前提となっている。

CS2 には、8 項目のセキュリティ機能要件と保証要件が規定されている。

(B)PP や ST の作成ガイドラインの標準化（ISO/IEC WD 15446）

ISO/IEC WD 15449 は、PP および ST の作成に関する指針を提供する国際標準案であり、現在 ISO/IEC JTC1/SC27 において策定作業が進められている。本国際標準案は PP および ST の作成者を対象としており、前述の表 12 および表 13 の各項目について、その内容の記述方法や記述する際のポイントなどを規定している。付録には、PP や ST を作成するためのチェックリストのほか、ファイアーウォール、データベース等の PP や ST が具体例として記載されている。

(C) JTC1 の PP 登録局要件の標準化（ISO/IEC WD 15292）

ISO/IEC WD 15292 は、JTC1 の PP 登録局（以下、JTC1-RA）およびその登録申請手続きに関する国際標準案である[21]。本国際標準案では、JTC1-RA は、登録申請の受付、申請書のレビュー、PP へ一意の識別子付与、受領通知、維持管理、公開、他の RA へ通知、利用手引きの発行を行うこととなっている。JTC1-RA は、登録を受け付けた後、「拒絶」、「PP への登録識別子の付与、審査」のいずれかを行うこととなっており、いくつかの拒絶理由が記載されているほか、登録申請者に対して拒絶に関する理由等の助言を与えることもある。

登録された PP は、一定期間後に登録の継続希望が行われない場合や、内容の欠陥が修復されない場合、「保留」の状態で管理されることとなっ

月に発表した「コンピュータセキュリティ基本要件・機能編」を、CC Version 2.0 および CS2 を参考にして改訂する方向で作業が進められている。

[21] 現段階では、PP の RA が JTC1-RA のみなのか、各国に RA を配置させることも可能なのかに関する記述は存在しない。

ている。ただし、一旦登録された PP は削除されることはなく、無効になった PP は「廃棄」のステイタスが付与されて管理される[22]。

5. CC に基づくセキュリティ評価スキーム CEM

(1)概説

CEM は、CC に基づくセキュリティ評価スキームであり、現在 CEMEB（CEM Editorial Board）において策定作業が進められている。CEM は、Part 1～Part 3 の 3 部から構成される予定となっており、現在 Part 1（概要と一般モデル）と Part 2（評価方法）のドラフトが公開されている[23]。

Part 1 では、セキュリティ評価を実施する際の原則や前提条件のほか、評価のモデルが記載されている。Part 2 では、情報セキュリティ関連製品・システムの評価方法が記載されており、TOE のレベル（EAL 1～7）に応じて、CC の Part 3 に規定されている評価項目について評価に必要な情報と評価者の行為が記載されている。なお、今後作成されることとなっている Part 3 では、評価結果を有効に利用するための手法について記載される予定であり、評価プロセスにおいて利用される資料や要求条件に関する説明が含まれることとなっている。

①評価の範囲

CEM における評価は、TOE となる製品・システム自身だけではなく、それらの品質を決定付ける製造工程に対しても実施される。例えば、ウォータフォールモデルに基づいて製品を設計・開発する場合、CEM の評価範囲は、基本設計書・要件定義書や上位・下位レベルの仕様書、ソースコード、テスト仕様書、概説書・マニュアル等、各開発工程において生産される資

---

[22] また、SC27 においては、以下の各点について検討が進められている。
①PP の評価に関する技術的内容に対する責任のあり方（RA ではなく、登録登録者が責任を持つべきとされている）
②RA を担う機関（現在フランスがノミネートされている）
③登録に必要な情報（評価レポートや認証書を入手するのに必要な情報＜識別情報、PP、新規・更新の別、状態、関連日付、登録者等＞を英語で記述。技術的な内容は自国語を用いて記述可能とされている）
④登録期間（5 年以上とされている）
⑤登録に必要な費用（登録時には登録料、登録の継続には継続料金を設定する方向で検討されている）。
⑥登録の状態（「登録」「保留」「廃棄」の 3 種類が検討されている）
⑦登録に関わる期間（登録可否審査は 3 ヶ月以内に行うほか、RA が廃棄を宣言して、実際に廃棄の表示が行われるには 18 ヶ月の期間を要することとされている）

[23] これらのドラフトは、NIST のホームページ http://csrc.nist.gov/cc/に掲載されている。

料が対象となる。さらに、開発工程の運営や管理に関する情報（品質管理やプロジェクト管理の情報等）も評価対象となる（図 6 参照)。

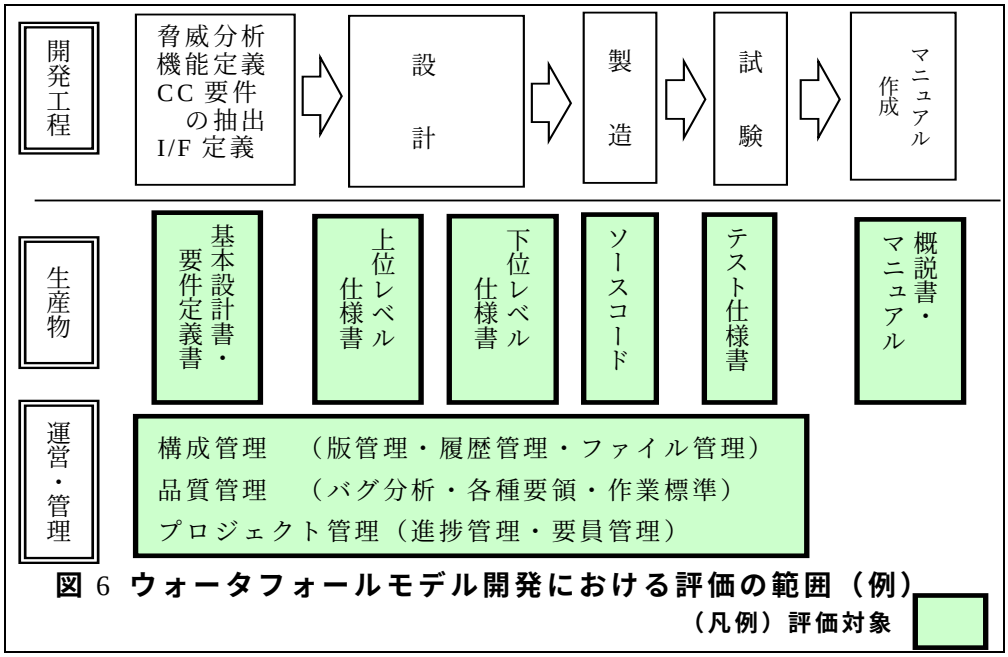


図 6 ウォータフォールモデル開発における評価の範囲（例）

②評価の当事者

評価を行う際には、「製品開発者（Developer)」「評価機関（Evaluator)」「監督機関（Overseer)」「調整機関（Sponsor)」「認定機関（Evaluation Authority)」の 5 者が関係する。

(A)製品開発者

製品開発者は、TOE を作成した主体であり、TOE の評価を評価機関に依頼する。要求に応じて、評価者に対して（または調整機関を通して）評価に必要な情報の提供や技術支援を行う。

(B)調整機関

調整機関は、評価機関が TOE を評価するために必要な調整を行う。例えば、評価を行うための事前合意の締結や、TOE に不具合や疑問点がある場合には製品開発者との仲介などを行う。

(C)評価機関

評価機関は、評価の実施主体であり、製品開発者や調整機関からの情報に基づいて、TOE が目標としているセキュリティの保証レベルに応じた評価を実施する。評価機関は、評価の結果を評価技術報告書（Evaluation Technical Report＜ETR＞）を作成して監督機関に提出する。

(D)**監督機関**

監督機関は、評価システムの運営について監督・監査し、評価スキームが正常に機能しているか否かをチェックする。また、評価機関の報告によって評価実施に不具合が生じていることが判明した場合には、評価機関に対して解決を促す等の措置を講じる。監督機関は、評価機関から提出された ETR を基に評価最終報告書（Evaluation Summary Report ＜ESR＞）を作成する。

(E)**認定機関**

認定機関は、監督機関から提出された ESR によって認定書を発行する。

③評価に利用される資料

評価対象を評価するために、次の 10 種類の資料が用いられる。各資料の概要は以下の表 14 の通り。

表 14　評価に利用される資料

資料	概要
ST	TOE の製造仕様書として利用された ST
PP	TOE が利用される分野の PP であり、ST が準拠したもの
Evaluation evidence	TOE の仕様書、プロジェクト管理に関する資料、テスト結果に関する資料等、設計・製造工程で作成された資料
Oversight deliverable	評価検査の結果として作成された資料
Interim verdict	評価機関が作成する中間判定の資料
Oversight verdict	評価機関が作成する検査判定の資料
Overall verdict	評価機関が作成する総合判定の資料
Observation Report	評価機関が作成する、評価の実行にあたって検出した問題点などの報告書
Evaluation Technical Report (ETR)	評価機関が作成する TOE に対する評価技術報告書
Evaluation Summary Report (ESR)	評価機関からの ETR にもとづき監督機関が作成する評価最終報告書

(2)Part1：**概要と一般モデル**

Part 1 では、セキュリティ評価を実施する際の 5 つの原則（適切、公平性、客観性、再現性、技術的正確性）と 4 つの前提条件（効率的な評価手順、最新の技術水準を反映した評価内容、既存の評価結果の効率的な利用、共通した用語体系の利用）が列挙されており、セキュリティ評価を実施する場合には、これらの原則や前提条件が満足していなければならないと説明されている。また、評価モデルの概要として、評価システムに関与する 4 つの主体（保証機関、評価機関、製品開発者＜評価依頼者＞、監査機関）の役割と責任に

ついて説明されている（図 7 参照）。

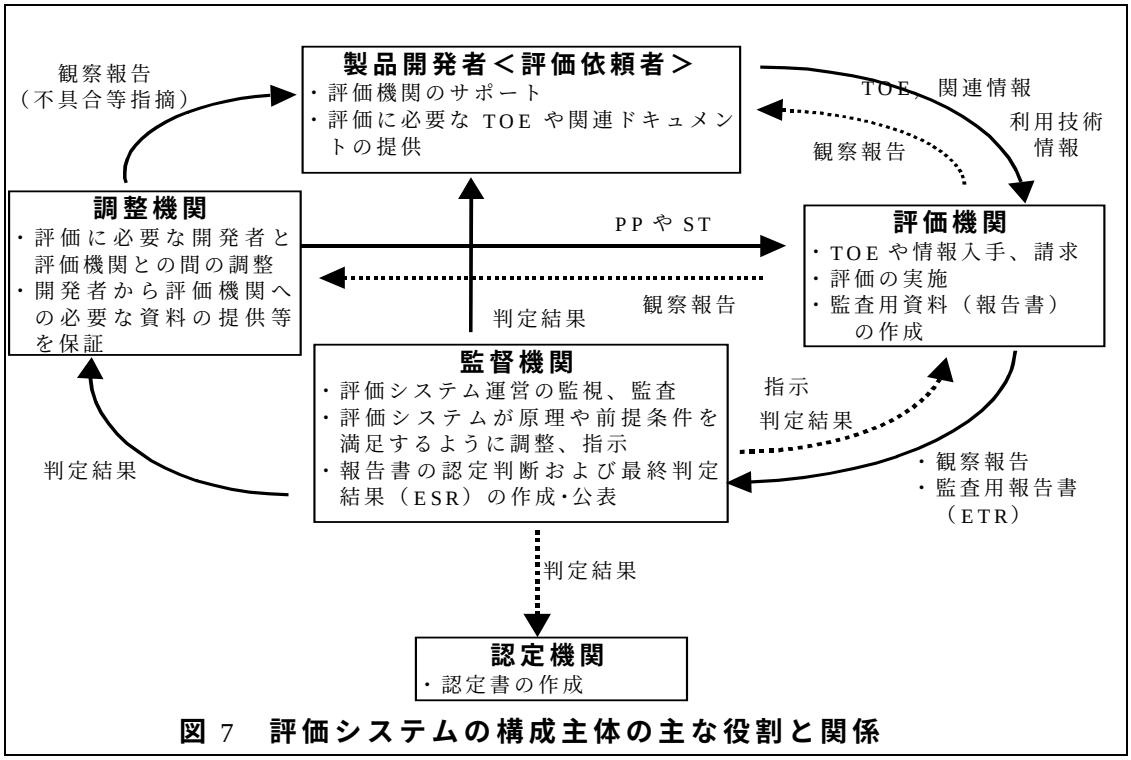


図 7　評価システムの構成主体の主な役割と関係

これらの主体がセキュリティ評価に関する原則と前提条件を満足するとした上で、準備、実施、結果の 3 段階によって構成される評価プロセスについて説明されている。各評価プロセスの概要は以下の表 15 の通り。

表 15　評価プロセスとその概要

	評価プロセス	概要
Stage 1	準備段階 ↓	調整機関と開発者は、評価機関に対して TOE に関する PP と ST 等の資料を送付する。これに対し、評価機関は、TOE の評価が可能か否かを分析し、PP や ST に不十分な点や改訂すべき点があれば通知。
Stage 2	↓ 評価実行段階 ↓	評価機関は入手した TOE や関連情報を基に評価を実施し、TOE に欠陥や問題点が存在する場合には、関連する情報を記録し、調整機関、開発者、監督機関に送付する。最終的な評価結果は ETR として記録され、監督機関に送付される。
Stage 3	↓ 結果作成段階	監督機関は、ETR を基に、評価が CC や CEM 等に準拠した形で適切に実施されていることを確認し、ETR が適正か否かを記載した ESR を作成する。ESR は、最終的な評価結果として調整機関、開発者、評価機関に送付されるほか、認定機関に送付される。最終的な認定書（Certification）は認定機関によって発行される。

6. 金融分野を対象とする PP の評価を巡る動き

金融分野において CC に基づくセキュリティ評価スキームを活用するためには、IC カードや ATM 等の情報セキュリティ製品・システムの金融業務用 PP を作成することが必要となる。現在、ISO/TC68 では、既存の PP を金融分野において利用可能か否かを評価するプロジェクトが進められている。また、わが国では、IC カード取引システム研究開発事業組合が、金融、交通、通信をはじめとする汎業界向けの IC カード用 PP を発表している。

(1)ISO/TC68 における PP 評価プロジェクト

①評価プロセス

SC2/WG5 では、以下の表 16 の手順によって既存の PP の評価・登録を行う方向で検討を進めている[24]。

表 16　ISO/TC68/SC2/WG5 における評価の流れ

フェーズ	内容
PP の評価申請	SC2/WG5 に評価の対象として PP が送付される。ただし、申請可能な PP は、各国の評価・認定機関によって認定・登録されている（または、その予定である）ものに限定される。PP は、WG5 メンバーもしくは各国代表団体（National Body）から申請できる。
PP の評価とコメント	PP の内容について審議が行われ、改訂すべき点があれば PP の申請者に通知する。申請者は、SC2/WG5 から寄せられたコメントを踏まえて PP の改訂を行い、その内容を SC2/WG5 に報告する。
TC68 メンバーによる投票	PP の評価・見直しの結果、SC2/WG5 が、金融業務用の PP として TC68/SC2 に登録すべきであると判断した場合、TC68 の規則に従って TC68 メンバーによって投票が行われる。PP は、DIS 段階の TR として投票に掛けられる。
PP の登録	投票において賛成多数の場合、その PP は、現在 SC27 において検討されている PP の登録手続きに沿った形で TC68/SC2 に登録される。

②IC カード関連の PP

現在評価の対象として SC2/WG5 に申請されているのは、①4 つの IC カード関連 PP、②1 つの ATM 用 PP、③2 つのファイアーウォール用 PP である。4 つの IC カード関連 PP のうち、3 つが Eurosmart[25]に参加している IC カードメーカーによって作成されたものであるほか、1 つが VISA によって

[24] SC2/WG5 における PP の評価のアプローチは、1999 年 9 月に開催された ISO/TC68/SC2 総会において了承されている。

[25] Eurosmart（European Smart Card Industry Association）：欧州における、IC チップ、IC カード、IC カード読取装置等、各種 IC カード関連企業の業界団体。IC カードの普及を目的として 6 つの Working Group を結成し、IC カードの標準化活動に加え、IC カード技術に関する研究開発や最新の技術情報を提供するフォーラムの開催等を行っている。

作成されたものである。各 PP の概要は以下の表 17 の通り。

表 17　IC カード関連の PP

名称	Smartcard Integrated Circuit PP	Smart Card Integrated Circuit with Embedded Software PP	Smartcard Embedded Software PP	VISA Smart Card PP
申請者（作成日）	Eurosmart（1998 年 9 月）	Eurosmart（1998 年 10 月）	Eurosmart（1998 年 11 月）	VISA（1999 年 5 月）
登録	仏・PP/9806	仏・PP/9809	仏・PP/9810	―――
評価対象	IC カード用チップ	専用ソフトウェア搭載の IC カード	IC チップ用ソフトウェアと関連データ	専用ソフトウェア搭載の IC カード
対象となる各製品のライフサイクル	専用ソフトウェアの納入、IC チップの開発・製造・品質検査、IC カード製造業者への配送、の各工程	専用ソフトウェアの開発、IC チップの仕様設計、の各工程	専用ソフトウェアの開発、チップへのソフトウェアの書込、の各工程	IC カードの使用および廃棄
保護対象となる資産	IC チップとその仕様・開発ツール、ソフトウェア、アプリケーション関連データ	IC カード、IC チップの仕様・開発ツール、ソフトウェア、アプリケーション関連データ	IC チップとソフトウェアの仕様・開発ツール、アプリケーション関連データ	―――
主な利用分野	金融、通信、交通、行政関連等	金融、通信、交通、行政関連等	金融、通信、交通、行政関連等	金融、通信、交通等
機能要件	・品質検査工程では 5 項目、品質検査工程以外では 12 項目を規定	・30 項目を規定。	・31 項目を規定。	・40 項目を規定。
保証要件 <保証レベル>	・3 項目を規定。＜EAL 4＞	・3 項目を規定。＜EAL 4＞	・3 項目を規定。＜EAL 4＞	・24 項目を規定。＜EAL 4＞

このように、IC カードの開発・製造・利用・廃棄のどの段階のセキュリティを確保するかによって、利用可能な PP は異なってくる。Eurosmart によって提案された PP/9806、PP/9809、PP/9810 はそれぞれ別の製造工程をカバーしているが、セキュリティ保証要件の保証レベルは EAL 4 で一致している。このため、一連の PP を併せて利用することによって、より広い製造工程におけるセキュリティ機能・保証要件をカバーできると考えられる。

一方、VISA の PP は主に金融業務での利用を想定して作成されており、IC カードの利用・廃棄の観点から必要とされるセキュリティ機能・保証要件が中心となっている。

③ATM 用 PP とファイアーウォール用 PP

ATM 用 PP は Cartes Bancaires[26]によって申請されているほか、2 つのファ

[26] Cartes Bancaires：フランスの 177 の金融機関（1999 年 7 月現在）からの共同出資によって設立された ATM ネットワーク運営会社。ATM ネットワークの運営とともに、加盟銀行間で利用可能なバンクカード「CB カード」の開発・運営等を行っている。

イアーウォール[27]用 PP が米国政府（NIST と NSA）によって申請されている。これらの PP の概要は以下の表 18 の通り。

表 18　ATM 用 PP およびファイアーウォール用 PP

名称	Automatic Cash Dispensers/ Teller Machines PP	U.S. Government Traffic-Filter Firewall PP for Low-Risk Environments	U.S. Government Application-Level Firewall PP for Low-Risk Environments
申請者 (作成日)	Cartes Bancaires （1999 年 3 月）	NIST, NSA （1998 年 9 月）	NIST, NSA （1998 年 9 月）
登録	仏・PP/9907	―――	―――
評価対象	CD, ATM ― CPU、現金払出部、IC カード読取部、キーパッドから構成。	Traffic-Filter Firewall	Application-Level Firewall
保護対象となっている資産	カード所持者の PIN、守秘・認証用暗号鍵、取引記録データ、残高データ、認証データ	―――	―――
主な利用分野	金融	米国政府機関のアプリケーション（「機密ではないが取扱に注意を要する情報」を取扱う場合）	米国政府機関のアプリケーション（「機密ではないが取扱に注意を要する情報」を取り扱い場合）
機能要件	・9 の機能要件を規定。	・20 の機能要件を規定。	・22 の機能要件を規定。
保証要件と保証レベル	・1 の保証要件を規定。 ・保証レベルは EAL 4。	・13 の保証要件を規定。 ・保証レベルは EAL 2。	・13 の保証要件を規定。 ・保証レベルは EAL 2。

(2)ICCS による IC カードサブシステム用 PP

日本国内における PP に関連する動きとして、IC カード取引システム研究開発事業組合（ICCS）[28]による IC カードサブシステム用 PP の作成が挙げられる。その概要は以下の表 19 の通り。

---

[27] ファイアーウォール：セキュリティ方針の異なるネットワークの接点に設置され、予め設定された取り決めに従ってネットワーク間でのアクセス制御を実施し、外部のネットワークからの不正アクセスを防止すると同時に、内部ネットワークからの不用意な情報流出を防止する情報セキュリティ製品。

ファイアーウォールは、利用される技術や設置される通信レイヤー等によって様々なタイプに分類することができる。米国政府から提案された PP の対象となっている Traffic-Filter Firewall は、ネットワーク層におけるパケットフィルタリング機能を有する Firewall として定義されているほか、Application-Level Firewall は、アプリケーション層で機能するファイアーウォールとして定義されている。

[28] ICCS（Research & Development Council for I.C. Card Commerce System）：1996 年 3 月に、日立製作所、沖電気工業、日本電気、三菱電機、大日本印刷等 IC カード関連メーカーを中心とする 47 社の出資によって設立された組合であり、情報処理振興事業協会の EC 推進事業の一環として行われた「EC 用非接触 IC カードに対応する汎用端末用リーダー・ライターユニットの技術開発」を受託することを目的として設立された。ICCS の概要やその研究成果については、http://www.iccs.gr.jp を参照。

表 19　ICCS・IC カードサブシステム用 PP の概要

名称	ICC Sub-System Protection Profile
作成者（作成日）	ICCS（1999 年 7 月）
評価対象	IC カードサブシステム（IC カード読取／書込装置の一部、IC カード、両者を接続する通信チャネルから構成） －　本 PP では、幅広い分野における IC カードを想定しており、必要最小限かつ一般的な機能が実装された IC カードおよび読取／書込装置を想定。このため、IC チップは、CPU、メモリー、I/O ポートから構成されるほか、IC カード読取／書込装置は、CPU、メモリー、2 つの I/O ポートから構成される。
PP がカバーする IC カードサブシステムのライフサイクル	ICC Sub-System の使用時 －　IC チップ、ソフトウェア、IC 読取／書込装置の製造等の諸工程は適用範囲外。
主な利用分野	特定されていない。
機能要件	・44 の機能要件を規定。
保証要件と保証レベル	・23 の保証要件を規定。 ・保証レベルは EAL 4。

本 PP では、評価対象が、IC カード、IC カードの読取／書込装置の一部、両者を結ぶ通信チャネルから構成される「IC カードサブシステム」という形態となっており、IC カードや IC チップ単体の PP とは異なっている。この点について、ICCS[1999]では、「利用される IC カード読取／書込装置の機能やセキュリティを考慮せず、IC カードのセキュリティを議論することはできない」と説明されている。また、IC カードサブシステムの利用時を主に想定してセキュリティ機能・保証要件が整理されており、保証レベルは EAL 4 となっている。利用分野は特定されておらず、金融、通信、交通をはじめとする幅広い分野に適用できるシステムが想定されている。

Ⅳ. 情報セキュリティ管理の評価・認定

本章では、情報セキュリティ管理に関するガイドラインとして、英国の標準 BS 7799 について説明する。情報セキュリティ管理のガイドラインとしては、BS 7799 以外に ISO/TR 13569 や GMITS が存在しているが、BS 7799 の特徴は、実際に BS 7799 に基づいて情報セキュリティが適切に管理・運営されているか否かを第三者機関が評価・認定するスキーム c:cure が準備されていることである。こうした第三者機関による評価・認定に関しては、TCSEC や ITSEC に基づく情報セキュリティ製品・システムの評価・認定や ISO 9000 シリーズに基づく品質管理の評価・認定[29]をはじめとして様々なスキームが存在している。しかし、情報セキュリティの管理・運営体制を対象とする評価・認定のスキームについては、BS 7799 に基づく c:cure 以外にはほとんど知られていない（BSI[1999]）。このため、BS 7799 は、評価・認定スキームを有する情報セキュリティ管理のガイドラインとして注目されている[30]。

1. 英国の情報セキュリティ管理のガイドライン・BS 7799

(1)BS 7799 の構成

BS 7799（Information Security Management）は、英国における汎業界向けの情報セキュリティ管理に関するガイドラインであり、BSI-DISC[31]によって作成された。BS 7799 は 2 つの Part から構成されており、Part 1 は情報セキュリティ管理に関するガイドラインであり、1995 年に作成・発表されている[32]。Part 2 は、Part 1 に基づく評価・認定スキームを実現するために 1998 年に作成・発表されており、組織の情報セキュリティ管理・運用体制を整理した文書「情報セキュリティ管理システム（Information security management

---

[29] ISO 9000 シリーズは、企業が製品・サービスを製造・提供する際の品質管理に関する基準・認証制度の国際標準規格であり、ISO において品質管理を検討する専門委員会 ISO/TC176 によって 1987 年 3 月に策定された。わが国では、ISO 9000 シリーズに基づく認定を実施する評価・認定機関の認可機関として、1993 年に日本適合性認定協会が設立されており、民間の評価・認定機関によって認証書が発行されている。

[30] 金融情報システムセンターのレポートによると、BS 7799 は、英国だけでなく、オランダ、カナダ、オーストラリア、ニュージーランド等でも採用されているようである（金融情報システムセンター[1999]）。

[31] BSI-DISC（British Standard Institute - Delivering Information Solutions to Customers）：BSI は科学技術全般における英国国内標準（British Standard）の策定を担当する組織であり、DISC は BSI の中で情報通信技術における標準化を担当する部署。なお、BSI は ISO 9000 等の評価・認定機関としても活動している。BS 7799 の関連情報や、BSI や DISC に関する情報は、http://www.bsi.org.uk/disc を参照。

[32] 1995 年に発表された Part 1 は、1999 年 4 月に一部改訂が行われた。改訂内容は、①デジタル署名や鍵管理等の暗号技術に関する解説や、②携帯電話・ファックス等の様々な通信手段の管理方法に関する解説が拡充されたこと、等である（BSI[1999]）。

system＜ISMS＞)」の内容、作成手順、管理方法を解説するものである。

(2)Part 1：情報セキュリティ管理に関するガイドライン

Part 1 では、情報セキュリティポリシーの作成、物理的なセキュリティ管理、情報システムへのアクセス管理等、情報セキュリティ対策を講じる際に検討すべき 10 の項目について解説されている。

BS 7799 Part 1 の構成

1. 情報セキュリティポリシー
2. セキュリティ管理のための組織体制
3. 資産の分類と管理
4. ユーザー管理
5. 物理的なセキュリティ
6. コンピューター・ネットワーク管理
7. システムへのアクセス管理
8. システム開発・維持管理
9. 業務継続プラン
10. コンプライアンス

①情報セキュリティポリシー

組織の情報セキュリティに対する姿勢を明確にする情報セキュリティポリシーを作成し､そのドキュメントを全役職員に配布する｡情報セキュリティポリシーには、少なくとも(A)情報セキュリティの定義・目的とその重要性に関する説明、(B)最高経営責任者による情報セキュリティ確保に対する明確なコミットメント、(C)情報セキュリティに関する研修プログラム、(D)情報セキュリティに関する各役職員の責務、(E)情報セキュリティの事故等が発生した場合の報告方法を明記する。

②セキュリティ管理のための組織体制

経営に関与する役員から構成される「情報セキュリティ管理フォーラム」を設立し、(A)情報セキュリティポリシーの承認・見直し、(B)情報セキュリティ対策に関する情報伝達・調整方法、(C)新しい情報セキュリティ手段の採用に関する審議・承認等を実施する。

③資産の分類と管理

セキュリティ対策の対象となる資産は、(A)情報資産（データベース、データファイル等)、(B)ソフトウェア資産（アプリケーションソフトウェア、システムソフトウェア等)、(C)物理的資産（コンピューター、通信製品、磁気媒体等)、(D)サービス（通信サービス、情報処理サービス等）に分類されることから、各々の資産に適した対策を講じる。情報資産については、必要とされる機密性、完全性、可用性に応じた管理を行う。

④ユーザー管理

情報システムのユーザー（役職員や外部業者等）に対して、情報セキュリティの重要性に関する認識を高め、自分の責務を自覚させるための研修を実施する。また、情報システム自体に事故が発生した場合等に速やかに関連部署へ連絡する体制を整備する。さらに、情報セキュリティポリシーや内部規則に違反したユーザーに対する罰則を設ける。

⑤物理的なセキュリティ

高い機密性を有する情報を管理するサーバー等が存在する施設を安全領域に指定し、入退室管理や装置・データの持ち出し管理等の必要な措置を講じる。また、予備電源の確保、ケーブル配線の管理、装置のメンテナンス等に配慮する。

⑥コンピューター・ネットワーク管理

(A)コンピューターやネットワーク関連製品の適切な操作方法や故障・事故発生時の対応方法、(B)コンピューターウィルス等を含むソフトウェアやファイルの検出・予防管理、(C)重要なデータのバックアップやログの管理、(D)暗号技術を利用した通信情報の機密性・完全性管理、(E)フロッピーディスク等記録媒体の管理等を講じる。

⑦システムへのアクセス管理

各情報システムやアプリケーションへのアクセス権限を各ユーザーに付与した上で、(A)ユーザーID とパスワードによるシステムへのアクセス管理や、(B)システムへのアクセス回数や時間等の使用状況のモニタリング、(C)無権限アクセスに対する罰則規定の設置等の措置を講じる。また、内部システムをインターネット等に接続する場合には、(C)ファイアーウォールによる外部ネットワークとの接続管理等を実施する。

⑧システム開発・メンテナンス

システム開発の際には、処理対象の情報の機密性や可用性等を考慮し、セキュリティ要件を明確にした上で、暗号技術の採用等いかなるセキュリティ機能が必要となるかを検討する。また、システムのメンテナンスを実行する際には、システム変更によるシステムのセキュリティへの影響の分析や、メンテナンスの記録管理等を実施する。

⑨事業継続プラン

災害や事故等の発生によって情報システムが利用不可能となった場合でも、事業遂行への影響を最小限に止め、事業を継続させるためには、(A)複数の業務における優先順位の決定、(B)様々なタイプの災害による潜在的なリス

クの分析、(C)事業継続プランの作成・テスト等を予め実行する。また、一旦作成された事業継続プランの有効性は技術革新や事業・組織体制の変化に伴って変化するものであり、プランを定期的に見直す。

⑩コンプライアンス

既存の情報システムの管理方法に関して、(A)関連法律（知的財産権や個人情報保護等）に対するコンプライアンス、(B)情報セキュリティポリシーに対するコンプライアンスが十分に守られているか否かを検証する。

(3)Part 2：情報セキュリティ管理システムの仕様

Part 2 は、BS 7799 に基づく情報セキュリティ管理体制の評価・認定を行うために作成されており、評価・認定の重要な資料となる ISMS の内容、作成方法、管理方法を解説しているほか、Part 1 の 10 項目が「詳細なセキュリティ管理手段」として列挙されている。

ISMS は、各組織が採用しているリスク管理方法や情報セキュリティ手段の内容を記述したものであり、各組織によって異なる。ISMS に記述される内容は情報セキュリティ対策の実施規定に対応し、ISO/TR 13569 における「情報セキュリティプログラム」の内容とほぼ対応している。ISMS の作成プロセスは以下の通り（図 8 参照）。

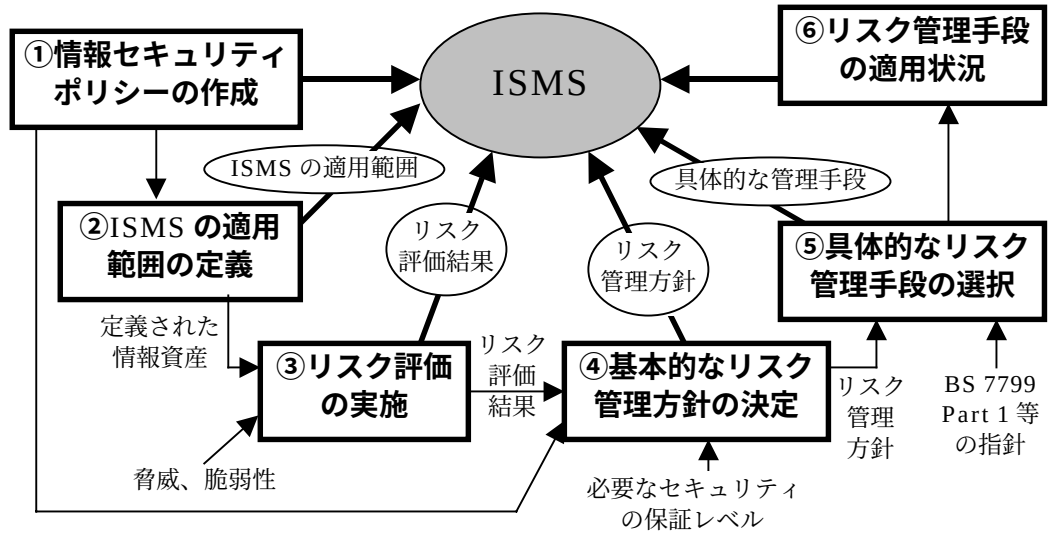


図 8　BS 7799 Part 2 における ISMS の作成手順

①情報セキュリティポリシーを作成する。

②ISMS の適用範囲となる情報資産を定義する。

③適用範囲内の情報資産に対して、潜在的な脅威や脆弱性をリストアップし、

リスク評価を行う。

④情報セキュリティポリシー、リスク評価結果、組織として最低限必要となる情報セキュリティの保証レベルを考慮した上で、基本的なリスク管理の方針（例えば、ネットワークを隔離することで内部システムのセキュリティを確保する等）を決定する。

⑤リスク管理方針に基づき、BS 7799 Part 2 に記載されている情報セキュリティ手段を参考にして、具体的なリスク管理手段を選択する。

⑥具体的なリスク管理手段に基づいて実際に実装した場合、その実装内容と、リスク管理手段の適用状況を記述する。

⑦情報セキュリティポリシー、ISMS の適用範囲、リスク評価結果、基本的なリスク管理方針、具体的なリスク管理手段、実装状況、リスク管理手段の適用状況の 7 項目をまとめて ISMS とする。

また、Part 2 では、一旦作成された ISMS は、技術動向や組織の改変等に伴って適宜アップデートし、その履歴を記録・保管することが望ましいとしている。さらに、実際のセキュリティ管理手段の運用が ISMS の内容と適合していることを証明する情報（監査記録、アクセス承認記録、情報システム施設への入退出記録等）を安全に管理することが望ましいとしている。

2. 情報セキュリティ管理システムの評価・認定の仕組み・c:cure

(1)c:cure の概要・枠組み

c:cure（The Accredited Certification Scheme for BS 7799）は、①BS 7799 に基づいて作成された ISMS の内容が十分か（情報セキュリティポリシーやリスク評価結果等が含まれているか）、②実際の情報セキュリティ管理の運用状況が ISMS の内容に適合しているかを、第三者機関が評価・認定する仕組みであり、1998 年 4 月から運用が開始されている（Owens[1998]）。

c:cure の枠組みは、(A)評価・認定機関のほか、(B)評価・認定機関を認可する UKAS、(C)評価手法の調査研究や国際標準との整合性確保等を担当する BSI、(D)UKAS や BSI の業務内容の指導・検査を実施する DTI から構成される。また、評価・認定機関は、(E)IRCA[33]から c:cure auditor としての認定を受けた審査員を採用することが必要とされている（図 9 参照）。

[33] IRCA（International Register of Certified Auditors）：品質管理等の審査員や研修機関を国際的に登録するための制度。IRCA の業務は、英国における品質管理関連の出版、研修、コンファレンス開催等を行う業界団体 IQA（Institute for Quality Assurance）によって行われている。

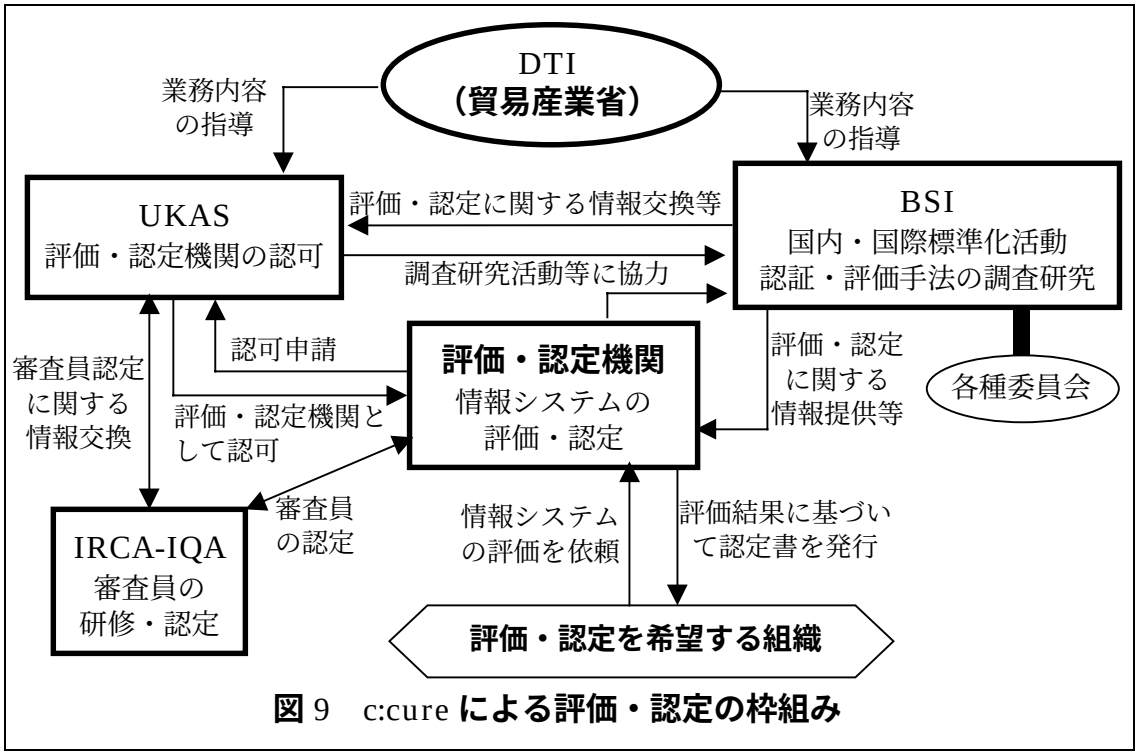


図 9　c:cure **による評価・認定の枠組み**

―　こうした c:cure における評価・認定の枠組みは、品質管理に関する認証制度の国際標準 ISO 9000 シリーズの英国における枠組みをそのまま流用したものである。英国では、ISO 9000 における審査登録機関（c:cure における評価・認定機関に対応）の認可を UKAS が担当しているほか、審査員についても、IRCA や IQA の資格認定等をうけることが要求されている。

BS 7799 および c:cure は英国標準であり、国際標準ではない。ただし、今後 BS 7799 および c:cure の評価・認定スキームが国際標準化される可能性もある。

(2)c:cure **の評価・認定プロセス**

評価・認定機関による c:cure の評価・認定プロセスは以下の通り（次頁の図 10 参照）。

①評価・認定機関の選択

評価・認定を受けることを希望する組織（以下、利用者と呼ぶ）は、認可を受けた評価・認定機関のリスト（UKAS が提供）から、評価・認定機関を選択する。

②評価・認定対象の範囲の報告

利用者は、評価・認定の対象となる情報システムの範囲を書面にて評価・認定機関に報告する。通常は ISMS の適用範囲と同一となるが、必ずしも同

一である必要はない。ただし、対象となる情報システムは ISMS の適用範囲に含まれることが必要である。

③**資料の提出**

利用者は、ISMS に関する資料に加え、事業内容、事業所の数・所在地、従業員数等の組織概要に関する資料、情報システムの仕様に関する資料等、評価・認定に必要となる資料を評価・認定機関に提出する。

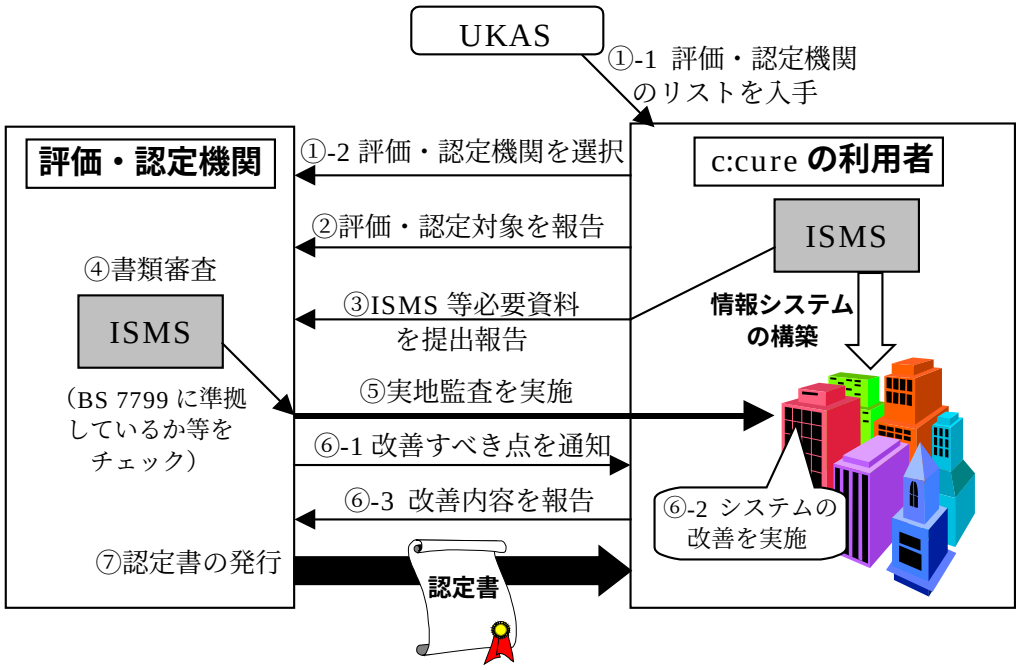


図 10　c:cure による評価・認定プロセス

④**書類審査**

評価・認定機関は、提出された資料に基づき、ISMS が適切に作成されているか否かを審査する。具体的には、情報セキュリティポリシーやリスク評価結果等が、①具体的なリスク管理手段の選択に反映されているか、②実装状況やリスク管理手段の適用状況と整合的かが審査される。

⑤**実地監査**

評価・認定機関は、予め利用者に通知したスケジュールに基づいて実地監査を実施する。評価・認定の対象となっている情報システムを実際に視察するとともに、管理・運用部署の責任者から実際の管理体制について説明を受ける。

⑥**問題点の指摘**

実際の情報セキュリティ管理の内容が ISMS の内容と適合しない場合、評価・認定機関は、利用者に対して問題点を指摘し、改善を促す。利用者は、

適宜システムの改善を実施する。

⑦**認定書の発行**

問題点が改善された場合、評価・認定機関は、利用者の情報セキュリティ管理が BS 7799 に準拠した ISMS に沿って適切に実行されていることを認定し、認定書を発行する。認定書には、認定された組織名や業務内容、認定を受けた情報システムの範囲、「評価対象の情報システムに関する ISMS が BS 7799 に準拠している」旨の文言、認定番号、認定開始日等が含まれる。認定書の有効期間は 3 年。

⑧**認定の更新**

認定書発行後、評価・認定機関は、年に 1 回程度システムの一部における情報セキュリティ管理の状況をチェックするほか（認定書発行時ほど大掛かりなものではない）、3 年ごとに実地監査を実施し、認定更新の適格性を検証する。なお、利用者は、大規模な組織改変やシステムの更新・変更を実施した場合、その詳細な内容について評価・認定機関に報告することを義務付けられる。

なお、評価・認定にかかる費用は、何人の審査員が必要か、評価期間はどの程度かによって決定されるため、評価・認定の対象となる組織の規模や業務内容に依存する。また、各評価・認定機関は、独自にサービスの価格設定を実施可能となっている。

3. BS7799 に基づく評価・認定を巡る動き

(1)評価・認定機関の認可と認定書の発行

1998 年 4 月に c:cure の運営が開始された後、1999 年 8 月 25 日時点で、UKAS から c:cure による評価・認定機関としての認可を取得しているのは DNV Quality Assurance 社[34]をはじめとする 3 社となっている。また、BSI をはじめとする 5 つの組織が、UKAS に評価・認定機関としての認可申請を行っている最中である[35]。

BS 7799 に基づく認定書は、1999 年 4 月までに、DNV Quality Assurance から 3 つの企業に対して発行されている（BSI[1999]）[36]。

---

[34] DNV（Det Norske Veritas）Quality Assurance 社：1864 年に設立された品質審査・認定会社（本社はノルウェー、従業員 5600 人、100 か国に支店を設置）。ノルウェー、英国、米国をはじめとする世界各国において、ISO 9001 や ISO 14001 等に基づく評価・認定機関として認可を取得。ホームページは http://www.dnv.com/。

[35] 評価・認定機関のリストについては http://www.c-cure.org/fcertific.htm を参照。

[36] 認定書の発行を受けたのは、経営コンサルティング会社の Business Link London City Partners 社と Insight Consulting 社、および、印刷会社の Wright Publications 社の 3 社。

(2)金融分野に関連する評価・認定の動き

金融分野における BS7799 の認定取得に関する動きとしては、英国最大の ATM ネットワーク LINK における情報システムの評価・認定が挙げられる（BSI[1999]）。LINK に接続されている ATM は、1999 年 8 月時点で英国内で約 25000 に達しており、英国内の全 ATM の約 9 割を占めている。LINK を運営している LINK Interchange Network 社[37]は、ATM を管理する情報システムの管理・運営体制の評価・認定を BSI に依頼しており、現在評価の最中となっている[38]。LINK Interchange Network 社は、BS 7799 に基づく認定を取得することによって、自社のシステム管理体制に対する信頼を高めることができるとしている。

[37] LINK Interchange Network 社：1986 年に、スコットランド銀行やバークレイズ銀行をはじめとする 34 の金融機関等の共同出資によって設立された英国国内の ATM ネットワーク運営会社。ホームページは、http://www.link.co.uk/。

[38] BSI は、1999 年 8 月 25 日時点では、UKAS に対して BS 7799 に基づく評価・認定機関の認可申請を行っている最中であり、正式には認可を受けていない。ただし、近々UKAS から認可を取得する見込みといわれており、認可を取得した後には LINK Interchange Network 社に対して認定書を発行することが可能になる（BSI[1999]）。

Ⅴ. おわりに

情報システムにおけるセキュリティレベルは、個々の情報セキュリティ製品のセキュリティレベルだけでなく、そのシステムの管理・運用体制等にも依存している。このため、一か所でもセキュリティレベルの低い部分が存在した場合、情報システム全体のセキュリティレベルの低下に繋がる可能性があることから、セキュリティを維持・向上させるためには、総合的な対策が必要となる。現在進められている情報セキュリティに関する評価・認定スキームは、既存の情報セキュリティ対策の達成状況について第三者機関から評価を受けるというものであり、高度な専門知識と豊富なノウハウを有する第三者機関による評価結果は、総合的な情報セキュリティ対策を検討していく上で有用な情報となる。

ISO/TC68 では、金融業務向け PP の評価プロジェクトを進めており、CC に基づくセキュリティ評価の枠組み整備に向けて積極的に活動している。欧米の金融業界においては、従来から、ISO/TR 13569 等の技術報告書や国際標準を利用しながら自社の情報システムにおける情報セキュリティ対策を講じるという姿勢が一般的であり、こうした取り組みは珍しいことではない。これに対して、日本の金融業界では、国際標準等を意識して情報セキュリティ対策が講じられてきたとは必ずしも言えないのが実情である。

現在進められている新しい情報セキュリティ評価・認定のスキームは、総合的なセキュリティ対策を進めていく上で有用なツールとなる。わが国においても、こうした動向に注目し、自社の情報システムにおけるセキュリティ対策を講じる際に、情報セキュリティ評価・認定のスキームを活用していくことも考えられよう。

以　上

参考文献

今井秀樹監修、宝木和夫、小泉稔、寺田真敏、萱島信著、『ファイアーウォール －インターネット関連技術について－』、情報セキュリティシリーズ第 2 巻、昭晃堂、1998 年 6 月

岩下直行・谷田部充子、「金融分野における情報セキュリティ技術の国際標準化動向」、『金融研究』第 18 巻第 2 号、pp.33-56、日本銀行金融研究所、1999 年 4 月

金融情報システムセンター、『金融機関等コンピュータシステムの安全対策基準』、1998 年 7 月

菅知之、「セキュリティ評価基準の動向」、1992 年暗号と情報セキュリティシンポジウム発表論文、SCIS92-10A、1992 年

――――、「海外の安全対策ガイドライン、国際標準から見た安全対策の調査・研究」、『金融情報システム』No. 216、pp.30-48、金融情報システムセンター、1999 年 6 月

British Standard Institution, “BS 7799: Information security management, Part 1. Code of practice for information security management systems,” February 1998.

――――, “BS 7799: Information security management, Part 2. Specification for information security management systems,” February 1998.

――――, “c:cure world, Helping you get the most out of BS 7799 - Information Security Management,” 1999.

Bull SC&T, Dassault A.T., Diebold, NCR, Siemens Nixdorf, and Wang Global, “Automatic Cash Dispensers/Teller Machines Version 1.00－Protection Profile,” Registered at the French Certification Body under the number PP/9907, March1999.

――――, De la Rue Card & Systems, Eurosmart, Gemplus, Giesecke & Devrient, Motorola Semiconductors, Oberthur Smart Card, and ODS, “Protection Profile Smart Card Integrated Circuit with Embedded Software Version 1.0－Common Criteria for Information Technology Security Evaluation,” Registered at the French Certification Body under the number PP/9809, October 1998.

International Organization for Standardization, “ISO/TR 13569 Banking and related financial services－Information security guidelines,” November, 1996.

――――――, “ISO/TR 13569 Banking and related financial services－Information security guidelines,” October, 1997.

――――――, “ISO/TR 13569 Banking and related financial services－Information security guidelines, Amendment 1,” December, 1998.

――――――, “Draft: ISO/TR 13569 Banking and related financial services－Information security guidelines,” August 19, 1999.

――――――, and International Electrotechnical commission, “ISO/IEC TR 13335-1, Information technology－Security techniques－Guidelines for the Management of IT Security－Part 1: Concepts and Models for IT Security,” 1997a.

――――――, and ――――――, “ISO/IEC TR 13335-2, Information technology－Security techniques－Guidelines for the Management of IT Security－Part 2: Managing and Planning IT Security,” 1997b.

――――――, and ――――――, “ISO/IEC TR 13335-3, Information technology－Security techniques－Guidelines for the Management of IT Security－Part 3: Techniques for the Management of IT Security,” 1997c.

————, and ————, “ISO/IEC TR 13335-4, Information technology－Security techniques－Guidelines for the Management of IT Security－Part 4: Selection of Safeguards,” 1997d.

————, and ————, “ISO/IEC TR 13335-5, Information technology－Security techniques－Guidelines for the Management of IT Security－Part 5: Safeguards for External Connections,” 1997e.

————, and ————, “ISO/IEC FDIS 15408-1, Information technology－Security techniques－Evaluation criteria for IT security－Part 1: Introduction and General Models,” 1999a.

————, and ————, “ISO/IEC FDIS 15408-2, Information technology－Security techniques－Evaluation criteria for IT security－Part 2: Security functional requirements,” 1999b.

————, and ————, “ISO/IEC FDIS 15408-3, Information technology－Security techniques－Evaluation criteria for IT security－Part 3: Security assurance requirements,” 1999c.

Motorola Semiconductors, Philips Semiconductors, Service central de la Sésurité des Systémes d’Information, Siements Semiconductors AG, SGS-Thomson Microelectronics, and Texas-Instruments Semiconductors, “Smartcard Integrated Circuit Protection Profile Version 2.0－Common Criteria for IT Security Evaluation Protection Profile,” Registered at the French Certification Body under number PP/9806, September 1998.

National Institute of Standards and Technology, “Security Requirements for Cryptographic Modules,” FIPS PUB 140-1, 1994.

————, “CS2 － Protection Profile Guidance for Near-Term COT（Draft Version 0.4）,” December 10, 1998.

————, and National Security Agency, “U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments Version 1.b,” September 1998.

————, and ————, “U.S. Government Application-Level Firewall Protection Profile for Low-Risk Environments Version 1.b,” September 1998.

Owens, S., “Information Security Management: An Introduction, An overview of the scheme for accredited certification for BS 7799,” British Standard Institution, 1998.

Research and Development Council for I.C. Card Commerce System, “ICC Sub-System Protection Profile Version 0.2,” July 1999.

Schlumberger, “Smartcard Embedded Software Protection Profile－Common Criteria for IT Security Evaluation,” Registered at the French Certification Body under the number PP/9810, November 1998.

VISA International, “VISA Smart Card Protection Profile Draft Version 1.6－Common Criteria for Information Technology Security Evaluation,” May 1999.